kpmg

Project Report

STRATEGIC STUDY OF RCMP ECONOMIC CRIME PROGRAM

Prepared for

Royal Canadian Mounted Police
Economic Crime Branch
Federal Services Directorate
1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

Attn: John Sliter
Project Manager

Submitted by

Garry Sears, Partner
Kate Jast, Principal
Geoff Golder, Principal
Catherine Caule, Senior Manager
Gregg Feltham, Manager
Margaret Beare, Senior Associate

Ottawa
September 4, 1998
46672/GS/03HR67/kc

+1

Contents

Executive Summary I

A. Report highlights I
B. Study process II
C. Trends and issues in economic crime II
D. Impacts of economic crime III
E. Feedback from stakeholders IV
F. Feedback from Commercial Crime Members V
G. Recommendations VI

I Introduction 1

A. Introduction 1
B. Project objectives 2
C. Mandate of Economic Crime Program 3
D. Study process, methodology and report structure 3

II External Trends And Issues 7

A. General Trends and Issues 7
B. Technology related trends and issues 23

III Impacts Of Economic Crime 33

A. Framework for describing and analyzing the magnitude and impacts of economic crime 33

Contents (cont'd)

B. Summary characteristics of the magnitude and impacts of economic crime 34

C. Current versus ideal positioning of the Economic Crime Program 56

IV Assessment Of The Program's Mandate And Associated National Interest And International Harmonization Issues 65

A. Clarity and focus of the Program's mandate needs to be sharpened 65

B. "National interest" in law enforcement focuses on public confidence in, and the integrity of, the national economic infrastructure 69

C. Determination of relative benefits gained by key players 76

D. Canada/US harmonization of enforcement efforts 85

V Stakeholder Feedback 93

A. Trends 93

B. Process 95

C. Communication and cooperation 96

D. Resource allocation 97

E. Human Resources 98

F. Technology 99

VI Commercial Crime Member Feedback 101

A. Process issues 101

B. Communication and cooperation 104

C. Resource allocation 104

Contents (cont'd)

D. Human resources 105

E. Technology 106

VII Recommended Organization Structure For Economic Crime 107

A. Key factors driving changes to Economic Crime 107

B. Current organizational model 108

C. Recommended conceptual organization model for Economic Crime 109

D. Evaluation of National Economic Crime Program Model against organization design principles 123

E. Rationale for moving to a National Economic Crime Program 125

F. Skills and competencies 131

VIII Resource Issues And Requirements 141

A. Economic Crime Program resources 141

B. Overall approach to resource management 142

C. Training strategy and resources 155

D. Technology resources 163

E. Resource requirements 167

F. Resource management policy issues 199

IX Recommendations...201

A. Impacts of economic crime and stakeholders' expectations regarding the future positioning of the Program 201

B. Recommendations relating to the national role and interests 202

Contents (cont'd)

C. High-level recommendations on Human Resources Management 206

D. High-level recommendations of Resource requirements 209

X Implementation Approach.. (NOT INCLUDED) 213

Appendices

A. List Of Participants in Individual Interviews or Group Consultations (NOT INCLUDED)

B. RCMP Mandate For Economic Crime

C. Organizational Design Principles

D. Other Organizational Options Considered

E. Possible Sub-activities

F. Senior Experts on Transnational Organized Crime: *40 Recommendations from Lyon G8 Conference*

G. Guiding Principles For Resource Allocation And Management

H. Resource Requirements Methodology And Assumptions (NOT INCLUDED)

I. Offence Activity Volumes

J. Bibliography

Executive Summary

A. Report highlights

The profile of economic crime is changing, both in Canada and internationally. Organized crime is playing a central role in the rise of economic crime around the world. The international justice community is pressuring all countries to increase their efforts in fighting the organized crime threat. In Canada, stakeholders are calling on the RCMP to do the same. However, the past decade of economic restraint, coupled with other factors such as the increase in economic crime activity and the complexity of jurisdictional issues, has reduced the effectiveness of the RCMP's Economic Crime Program. Today, stakeholders, as well as RCMP members, are dissatisfied with the RCMP's performance in this area and want to see dramatic improvements.

Economic crime is a serious problem for Canada. While its impact is subjective and difficult to measure, the magnitude of economic crime in Canada is valued at between $2.1 and $3.1 billion. Canada's economy depends on the integrity of its underlying business activity and therefore requires strong and effective control over economic crime.

Stakeholders in Canada believe that the RCMP must be equipped to combat economic crime that is national and international in scope. They also believe that the RCMP has a very limited capability to carry out the increasing number of national and international economic crime investigations and other supportive activities. This reduction in RCMP capability in recent years is having serious repercussions. While stakeholders have expanded their monitoring and investigative activities, the increased reliance on administrative penalties and civil remedies is having declining success in controlling the activities of organized crime groups. In short, a loss in the deterrent effect has occurred. Organized crime groups have expanded their activities.

RCMP commercial crime members are also frustrated and distraught over their inability to deliver an effective service. They view the existing human resources policy as a major impediment to the motivation of investigators and the retention of expertise.

It is time for major change. It is recommended that the RCMP adopt a new National Economic Crime Service Line model that will provide for the delivery of a more effective national service. It is also recommended that the human resources complement be increased by almost 100%, at a total cost of approximately $100 million. The RCMP should also adopt a specialist human resource policy and recruit new investigators with enhanced skill levels that are required to effectively handle the investigation of complex economic crimes.

B. Study process

In late 1997, the Director, Federal Services Directorate, identified a requirement to conduct an intensive strategic study of the RCMP's Economic Crime Program. The overall objective of this study was to review the structure, roles and responsibilities of the Economic Crime Branch. In February 1998, KPMG Consulting was contracted to conduct an independent, strategic study.

The overall objectives of the study were to recommend an appropriate organizational structure for the Economic Crime Program, to identify the level of resources required to fulfill its mandated responsibilities and to identify the skill requirements for the required positions.

KPMG carried out this study under the general direction of a project steering committee consisting of representatives of the RCMP's Economic Crime Program at Headquarters. The findings and recommendations contained in this report are based on KPMG's independent fact finding and analysis. The final report was submitted in August 1998.

C. Trends and issues in economic crime

The RCMP's mandate for Economic Crime covers the following types of crime:

- Commercial fraud.
- Securities fraud.
- Telemarketing fraud.
- Internet fraud.
- Unauthorized use of computers/mischief to data.
- Theft of telecommunications.
- Fraud related to selected Federal statutes and programs (focusing on fraud related to Employment Insurance, tax avoidance, criminal bankruptcies) and corruption or financial theft cases where the Government of Canada is the victim.
- Currency counterfeiting.
- Payment card fraud.

The profile of economic crime is changing rapidly. No longer limited to the realm of petty counterfeiters and fraud artists operating in a single geographic area, the tremendous profit potential and the perceived low risk of retribution from victims and police have lured new, often highly sophisticated elements of society into economic or "white-collar" crime. Of special concern is the fact that countries around the world are experiencing a rise in organized crime involvement. Experts interviewed during this study have stated that the most important enterprise crimes in the future will be international financial fraud, commercial fraud, money laundering and tax evasion.

The rapid proliferation of information technology and other sophisticated technologies has facilitated the activities of organized crime. For example, a shift is occurring from basement counterfeiting operations to sophisticated mass production of forged currency, cheques, transaction cards and bank drafts by international criminal groups. Technology also enables these traditional criminals to expand their activities by weaving in white collar crimes such as money laundering and tax evasion. Furthermore, Canada's electronic information infrastructure supports every sector of the economy. These sectors are connected to each other in a complex network of interdependence. This interlinked infrastructure is vulnerable to sabotage. The U.S. has responded by creating a National Infrastructure Protection Centre, to serve as that government's lead mechanism to responding to potential infrastructure attacks.

Police forces around the world face difficulties in coping with the growing volume, complexity and internationalization of economic crime activity. The mechanisms that exist today for the conduct of joint police investigations that cut across jurisdictional boundaries are considered inadequate for dealing with transborder crimes. Within Canada, confusion often arises in such areas as federal versus provincial or local jurisdiction over economic crimes.

The past decade of financial restraint has seriously affected police budgets. As a result, there has been a rapid growth in the provision of security and investigative services by private agencies. While this trend has the positive benefit of the formation of numerous public/private partnerships, a number of important issues have also surfaced, such as differing mandate and priorities between the public and private sector.

In addition, the pressure for increased police accountability has profoundly affected how the police must carry out their investigative activities. For example, the increased requirement for disclosure has dramatically increased the administrative burden placed on investigators, thereby reducing the amount of time they can devote to investigative work.

Finally, the international community is pressuring countries, including Canada, to "pull their own weight" in the development and enforcement of economic crime laws.

D. Impacts of economic crime

KPMG's research on the magnitude and scale of the above types of economic crime shows that the sums involved—be they losses to individual consumers and investors or large organizations—are substantial. The total estimated magnitude of the value of the economic crimes we analyzed is at least $2.1 billion to $3.1 billion, plus unknown amounts for emerging, hard-to-value crimes such as Internet fraud and computer crime.

The experts we interviewed in assembling the impacts data believe that current RCMP resources are preventing the Economic Crime program from achieving its mandate. As a result, many organizations have had to expand their monitoring and investigative activities. They emphasized, however, that it is not possible, nor desirable, for stakeholders to take over the full range of activities that the program is capable of delivering.

The deterrence effect of the RCMP's Economic Crime program has been reduced in recent years due to increases in the volume of economic crime and the reductions in RCMP resources. This has had the effect of encouraging economic crime groups to expand their activities in Canada, which has led to increased financial losses for organizations and individuals. In addition, organizations and regulatory agencies have relied more upon the application of administrative penalties and civil remedies as a way of limiting the incidence of economic crimes. However, organized crime groups have continued, and expanded their operations, because the potential for significant financial returns outweighs the risk of criminal prosecution.

E. Feedback from stakeholders

During the course of this study, some 150 stakeholders representing federal and provincial governments, financial institutions and private sector corporations were consulted via personal interviews and focus groups.

Overall, stakeholders are dissatisfied with the service provided by the RCMP's Economic Crime Program. They stated that they see no national vision or direction for the program. They view the end-to-end process—i.e., from the determination of criminal activity to the conduct of investigations and the judicial process—as dysfunctional. They stated that the response rate of the RCMP is neither timely nor efficient. They indicated that once they submit a case to a Commercial Crime Section, they can wait weeks or months just to obtain a decision as to whether the case will be investigated. They also stated that the lack of leadership and management focus has eroded the capacity of the program over time. Symptoms include a continual decline in resources and fragmentation in levels of authority and accountability. They believe there is insufficient communications between the program and stakeholders. Notwithstanding their major concerns about the state of the program, they are anxious for more consultation and are willing to partner with the RCMP to expedite investigations.

Stakeholders are of the opinion that the Economic Crime program is under-resourced. While stakeholders have increased the resources they dedicate to dealing with the growing economic crime problem, they stated that the RCMP's program is currently resourced to address crime levels that existed about a decade ago.

F. Feedback from Commercial Crime Members

Many of the issues raised from the many RCMP Commercial Crime members we interviewed echoed the views raised by stakeholders. Members are emotionally distraught not only over the ongoing cutbacks, but also by the overall poor state of the Economic Crime program. Specifically, members are concerned that no national direction, strategy or national standards exist for economic crime. Management practices are ineffective and inconsistent from region to region. They believe that each area of the country is "doing its own thing," resulting in an inconsistent approach to service delivery. They see positions remaining vacant over long periods of time while investigators are spending long hours on cases and rejecting other viable cases due to lack of resources. Coupled with going reductions and ineffective management practices, members spend a disproportionate amount of time on administrative and clerical duties, when they should be focusing their effort on their investigative duties. In addition, they stated that they spend considerable time on investigations and special assignments outside of Economic Crime. While everyone agreed that as part of the duties of a national police force they should participate in these types of activities, no provision is made for continuation of ongoing cases.

They also believe that the program is stuck in a reactive, crisis management mode. They believe, as do stakeholders, that the program should be placing more emphasis on prevention and education.

Members are very concerned about the systemic human resources management problems which have long existed within the RCMP. They are frustrated with the skill levels of investigators, the lack of resources and the lack of commitment to learning and development, and the inability of the program to attract or retain qualified staff. Members point to the absence of a career path within the program and see an ongoing exodus of capable individuals to other RCMP programs or to external organizations with more effective recognition and rewards practices.

In summary, members see little or no evidence of senior management support for the Economic Crime program and believe that, if nothing changes, the program will die a slow, but certain death.

G. Recommendations

1. Establish a National Economic Crime Service Line

Several organizational models for the Economic Crime Program were discussed in workshops/focus groups held across the country. Although each option has its strengths and deficiencies, the option that addresses the most critical current as well as future needs is a National Economic Crime Program/Service Line, reporting to the Director of Federal Services.

While it is recognized that this recommended model differs from the recent RCMP trend towards decentralization, the rationale is justified on the following grounds:

- **Stakeholders and members both stress a national focus is required**—The national model will facilitate more effective management of national programming and resourcing. It will focus on key business activities by establishing a consolidated, cohesive and proactive approach to federal economic crime investigation, education and prevention.
- **Canada is perceived as a safe haven for organized crime**—The current lack of a national program puts Canada increasingly at risk of not being able to address the growth in economic crime from both national and international sources.
- **Our political leaders have committed to increased international partnering**—Internationally, other countries are looking to Canada to provide both a single point of contact in the fight against economic crime, as well as an effective decision maker to be represented around the table where international agreements are forged.
- **The Economic Crime Program must address systemic human resources management issues**—A national program would be better positioned as a united voice to address the many HR issues facing the program.
- **A more flexible management model is required**—Today, Commercial Crime Sections are subject to the changing needs of the local management infrastructure with little or no control over either financial or human resources. The Economic Crime Branch in NHQ has little or no say in the allocation of resources because it has no funding authority.

2. Provide the program with sufficient resources

In order for the Economic Crime Program to meet its mandate and its many challenges, it must have sufficient resources. In 1997-98, 475 FTE's were allocated to the program, a reduction from 507 in 1996-97.

In 1999, we estimate that the resources required to meet the workload for new cases would be 917 FTE's, which is forecast to increase to 1,215 FTE's in 2003. The financial resources required for 1999 would be $102.41 million.

While the incremental requirement of about 410 FTE's for 1999 may seem huge at first glance, we believe it is reasonable, particularly given:

- The historical and projected growth rates for economic crime identified by this study.
- The increasing complexity of cases which require more resources.

3. An increase in skill requirements is required for entry into the program

The National Economic Crime program should be defined as a specialized program requiring specialized skills. Minimum requirements should be established to guide recruitment and selection of individuals for the program, as well as for progression within the program. For new recruits for example, the minimum requirements could include a combination of an appropriate educational degree in business administration or related area, plus one to three years of relevant industry experience.

4. Enhance the Economic Crime mandate

A clear mandate for the National Economic Crime program is essential, as it can provide the ground rules for case selection decisions. We recommend that the following enhancements be made to the December 1997 mandate:

- Anticipated outcomes, not outputs, need to be clearly stated.
- The program's key stakeholders need to be identified.
- Although investigations are central to the program's operations, supporting capabilities also need to be highlighted.
- A revised "national interest test" needs to be incorporated (see recommendation #6).

5. The program should maximize its impact by focusing on certain types of crimes and activities

In order for the program to maximize the impact of any increases in the resources made available, it will need to focus on certain types of crimes and activities, working in partnership with stakeholders. Based on stakeholder feedback, we suggest that emphasis be placed on the following areas:

- Cases involving organized crime groups that account for significant losses or disruption. "Go after the big guys and send a strong deterrence to the small guys."
- Cases that have national and international components and are typically more complex and require higher levels of technical expertise, which are often not available in provincial or municipal forces.
- Cases that respond to emerging new threats and risks, in order to slow the spread of new criminal approaches and to ensure that the RCMP stays ahead of the game.
- The development of a stronger intelligence capability and increased sharing with stakeholders, leading to a more proactive approach in combating economic crime.

6. Enhance the "national interest test"

The program should incorporate a revised national interest test into its mandate. The following economic crime activities are likely to have the greatest impact on the national interest in law enforcement:

- Crime activities that:
    - Involve economic crime groups that account for significant losses or disruption.
    - Involve large scale, systemic fraud, computer crime or other types of economic crime.
    - Have regional, national and/or international dimensions.
    - Require higher levels of expertise and specialized knowledge to investigate, due to their complexity.
    - Respond to emerging threats and risks.

We also recommend that a "program and case priorities group," composed of a small number of program managers, be established to resolve questions regarding the assessment of certain cases and to regularly review the working of the national interest standard and results achieved.

7. Address certain human resources management issues

Several human resources management issues were raised repeatedly during our consultations, including the problem of staff attraction/retention, the lack of a career path within economic crime and the hierarchical promotion methods.

We provide the following high level conceptual recommendations that should be considered by RCMP senior management:

- Specialization—Economic Crime should be set up as a specialized program. The program requires individuals with not only general competencies, skills and knowledge, but also additional skills and knowledge that are specific to the program.

- Staffing/recruitment—The process of recruitment and staffing needs to be improved. Line/operational managers and human resource specialists both have specific roles and responsibilities in this process. The former identify their needs and the latter help managers to address these needs. Human resource specialists provide expert advice, guidance and design processes in support of effective management decision making. However, they do not make any final decisions with respect to the ongoing management of people and programs.

- Career streaming/succession planning—The National Economic Crime Program should provide a viable and flexible career path to retain qualified members and facilitate effective succession planning.

- Classification/promotions/reward-recognition—The "ranking" of positions was highlighted as a major problem. Members are currently unable to progress within the program unless a higher ranked position is available. Two options are suggested:

  - Option 1—Make all positions within the program "special agent" status.

  - Option 2—If the rank system were to be maintained, set up a parallel specialized rank structure.

8. Establish a resource management framework

A resource management framework is required to address the program's overall resource management system and to establish an appropriate accountability framework. Such a framework would allocate and support the control of, and accountability for, resource management and consumption between headquarters and the field.

I

Introduction

A. Introduction

The Federal Services Directorate of the Royal Canadian Mounted Police (RCMP), located at the National Headquarters in Ottawa, is responsible for the management of several national programs, including the Economic Crime Program. The Directorate has a number of branches, one of which is the Economic Crime Branch, which, in turn, has three sections: Commercial Frauds and Securities; Federal Section and Projects; and, Technological Crime.

The number of Regular Members within the Economic Crime Branch has significantly decreased over the past few years, as a result of internal RCMP re-organizations and federal government downsizing and economic restraint. However, over this same time frame, there has been significant growth in the volume and complexity of economic crime in general, as well as in the methods and capabilities of the perpetrators of such illegal activities.

At the inception of the Economic Crime Program in the mid-1960's, the initial mandate was quite clearly delineated and therefore relatively easy to define. The subsequent years saw a number of major changes in the types of criminal activities that were also perceived to fall within the mandate of the program, introducing a degree of ambiguity into the program's actual mandate. It is probably fair to say that the RCMP's role and responsibilities in this quickly changing field are not clearly defined at present. This lack of clarity has continued to the present day, as the definition of RCMP roles and responsibilities—as distinct from those of other law enforcement agencies—has not kept pace in this rapidly changing field.

The operational arm of the Economic Crime Branch consists of a number of Commercial Crime Sections (CCS), situated in a number of the larger cities across Canada at both the federal and provincial level—leading to issues over control of these resources.

In late 1997, the Director, Federal Services Directorate, identified a requirement to conduct an intensive strategic study of the Economic Crime Program. The overall objective of this study was to review the structure, roles and responsibilities of the Economic Crime Branch, with a special emphasis, during the initial study phase, on the

Technological Crime Section. In February 1998, KPMG Consulting was contracted to conduct the independent strategic study of the Economic Crime Program.

B. Project objectives

The overall objectives of this study were to recommend an appropriate organizational structure for the Economic Crime Program, to identify the level of resources required to fulfill its mandated responsibilities, and to identify skill requirements for the required positions. More specifically, the Terms of Reference for this study identified several primary objectives (PO's). These are:

PO-1 Impacts on Canadians of economic crime—Any attempt to determine the level of resources that the RCMP should devote to economic crime requires an assessment of the current and prospective nature and extent of the problem itself. Stakeholders were also to be asked for their views on the impacts on Canada should RCMP resources not be able to carry out the Economic Crime program mandate.

PO-2 Benefits analysis—The study was to develop a methodology for identifying the relative benefits gained by the key players from RCMP activity, at the federal and provincial levels, and hence a means of more accurately allocating the costs of the Economic Crime Program amongst its beneficiaries.

PO-3 Appropriate resource levels and organizational structure—The project was to determine the resources and skills sets required to deliver the mandate, and to recommend the preferred organizational model.

PO-4 National role and interests—To clearly define what is meant by the "national role and interests" of the Economic Crime Program. This was to include a clarification of what economic crime activities affect the national interest and therefore fall within the mandate of the program.

PO-5 Canada/U.S. harmonization—The increasing globalization of economic crime requires that police forces in various countries must harmonize their strategies and programs. While multilateral negotiations have progressed steadily, a priority for Canada is to continue to harmonize its efforts with the U.S. The study was to obtain feedback from stakeholders on the appropriate role for the RCMP.

In addition, the Terms of Reference identified a number of secondary objectives (SO's), which were to be examined but not at the expense of allocating sufficient effort to the primary objectives. The secondary objectives are:

SO-1 **International approaches**—To review the economic programs of other countries, such as the U.K. and U.S., and to assess whether their approaches could be applied or adapted to the RCMP. A specific goal was to obtain information on any available resource requirements methodologies.

SO-2 **Coordination with other police agencies**—To examine process and roles with a view to improving the current assignment of investigative resources and the coordination of roles between departments and agencies. This was to include such issues as the tasking of investigative resources, coordination with other agencies and leadership issues for all aspects of the program.

SO-3 **Public concern with technology crime**—To identify, to the extent possible, the degree to which Canadians, given the growth in the use of information technology and its criminal exploitation by organized crime, are concerned about this issue and the ability of the RCMP to carry out its enforcement responsibilities.

C. Mandate of Economic Crime Program

The mandate of the Economic Crime Program was updated in December 1997 and forms the basis for this strategic study. Some of the key elements of this new mandate include:

- A recognition that the RCMP has an obligation to respond to Economic Crime issues where the interest of the Government of Canada and Canadians are at stake.
- A recognition that the deployment of Federal resources to conduct interprovincial or international investigations under the *Criminal Code of Canada*, is acceptable in cases where the investigation satisfies a "national interest standard".
- A recognition that the RCMP must provide the highest quality service through dynamic leadership, education, and technology in partnership with the communities that it serves, and that the RCMP is widely recognized and respected for its technical and investigative expertise in specialized law enforcement.

D. Study process, methodology and report structure

This study was undertaken by KPMG consultants specializing in government strategy, economic analysis, organizational development and resource requirements analysis. Following a public tender process, KPMG commenced the project in late February 1998.

KPMG carried out its fact-finding and analysis under the general direction and guidance of a project steering committee consisting of several representatives of the RCMP's Economic Crime Program at Headquarters. This Committee assisted the consulting team by clarifying the study requirements and objectives, and facilitating access to information and contacts within the RCMP.

A key element of the study was the necessity for objectivity and independence. KPMG believes this requirement has been met. The findings and recommendations contained in this report are based on our independent fact-finding and analysis.

The study was divided into two phases. Phase I focused on Technological Crime, while Phase II was broadened to encompass all aspects of the Economic Crime Program.

The first deliverable of the study in Phase I was an analysis of the main trends and issues affecting the Economic Crime Program, with a particular focus on technological crime, as well as the identification of the key internal RCMP issues affecting its capability to deliver its program. The lead consultant in preparing this deliverable was Dr. Margaret Beare from York University, a recognized authority on the subjects of economic crime trends and on organized crime. This paper is contained in Chapter II of this report.

Phase I also involved our assessment of the RCMP mandate for Economic Crime (PO-4), which is contained in Chapter III. This chapter also summarizes the findings on the national interest test (PO-4), and the Canada/U.S. harmonization issue (PO-5).

Our analysis of the magnitude and impacts of economic crime (PO-1) is found in Chapter IV. The chapter provides estimates of the value of economic crime by type of crime (e.g., telemarketing fraud, securities fraud, Internet fraud, payment card fraud, telecommunications theft). This analysis involved an extensive literature review and interviews with representatives of various economic sectors, including telecommunications, securities, banking, and information technology.

A key methodological component of the study was the conduct of an extensive interview program, both within the RCMP and with stakeholders (a listing is provided in Appendix A). Personal interviews and roundtable discussions were held in many RCMP Divisions across Canada as well as at Headquarters. In addition, a 1 ½ day workshop involving Technological Crime program representatives was held in Toronto in April 1998. The feedback we received from stakeholders is summarized in Chapter V, while the feedback from RCMP Members is contained in Chapter VI.

Phase I involved the development of various options for Technological Crime program, which were further reviewed and assessed during Phase II for the entire Economic Crime Program. Our preferred option for the Economic Crime Program (PO-3) is contained in Chapter VII, and the entire set of options we analyzed is found in Appendix D.

Chapter VIII contains our resource requirements methodology (PO-3), as well as our recommended resource levels for the Economic Crime Program.

The three study secondary objectives were also investigated. SO-1 (international approaches) involved interviews with representatives of police agencies in the U.S., U.K. and Australia. Information on their resourcing strategies was incorporated into the study's resource requirements analysis (Chapter VII). Issues of inter-agency co-ordination (SO-2) received comment from stakeholders (Chapter V). Finally, SO-3 (public concerns with the use of technology in economic crime) is addressed in the Trends and Issues paper (Chapter II).

Finally, we developed an implementation plan for the recommended organizational option, which is contained in Chapter IX.

The main findings and recommendations of the study were presented at the Halifax Economic Crime POWPM in June 1998. The final study report was submitted in August 1998.

6

II

External Trends And Issues

This chapter presents a number of the key *external* trends and issues facing the RCMP's Economic Crime Program. These themes were identified through a broad-based literature review, supplemented by a series of interviews with representatives of the RCMP's Economic Crime Program, as well as selected Program stakeholders. The chapter is broken into two sections: General Trends and Issues and Technology related Trends and Issues.

A. General Trends and Issues

Seven major external trends have been identified:

- The profile of economic crime is changing.
- Reduced fiscal resources are forcing policing programs to realign the level and type of services they provide.
- Funding bodies are becoming increasingly involved in setting policies and priorities for law enforcement agencies.
- Police forces are losing their traditional "monopoly" over policing services.
- Increased demands to account for police actions have added to the workload of investigators.
- The international community is pressuring countries to "pull their own weight" in the development and enforcement of laws that relate to economic crime.
- The public perceives economic crime as a lower priority than physical/violent crime.

The paragraphs below explore each trend in turn, highlighting various facets of each trend, as well as implications for law enforcement services.

1. The profile of economic crime is changing

a) Economic crime is becoming a target growth area favoured by organized crime

> *"Diversity and change in organized crime activities have occurred because...the dollar amounts in criminal enterprises earned from commercial crime exceed that earned in drug trafficking."* (Carter, 1997, p.10)

> *"The traditional distinction between illicit and legitimate activities, with reference to organized crime, is becoming less evident in the modus operandi of organized criminals. At the same time, the distinction between what is criminal and what is not is becoming more and more vague. ...Organized crime and economic crime become more closely linked and the future trends of organized crime tend towards those productive activities where opportunities are big, risk is lower and highly complex organizations are required".* (Savona, 1997b, p.3)

Economic crime is no longer limited to the realm of petty counterfeiters and fraud artists operating in a localized area. The tremendous profit potential and perceived lower risk of retribution from victims and policing agencies have lured new, often highly-educated, elements of society into criminal schemes that are frequently characterized as "white collar crime". The potential gains become even more lucrative (and difficult to investigate) when scams involving multiple players spread across local and international borders are organized.

Recent studies have drawn attention to this trend, suggesting, for example, that while fraud is an ancient type of criminal enterprise, countries around the world are experiencing a recent evolution in the organizational aspect of fraud. As Ernesto Savona, Director of TRANSCRIME states *"...fraud against the community is not a question of petty pilfering, but of large scale organized financial crime"*. (1997a, p.2)

Criminal elements involved in major fraud in large Canadian cities are well organized, multilingual and "high-tech". In some cases, for example, the perpetrators possess intelligence training from former military regimes.[1] The policing of criminal groups which originate in countries of Eastern Bloc,

---

[1] *Source: "The Changing Face of Corporate Fraud" in* ***Canadian Manager****, V22N3, pp. 12-13, Fall 1997*

Africa and Asia, therefore, poses unique challenges in terms of the additional language and technical skills required.

Professor Savona provides a number of compelling examples of the "organization" behind the fraud cases:

- A counterfeit industry that is ab[illegible]produce credit cards that are of better quality than the genuine cards they are copying.

- Concerns of the American Bankers Association (ABA) that the criminal use of computer technology has resulted in extensive counterfeiting of corporate cheques, bonds, securities and negotiable instruments, plus counterfeit access devices and telecommunications identification documents.

- Counterfeit currency in Western Europe that has tripled during the years 1991-1993.

- Criminal organizations in the European Union are tending to "invest" their laundered and unlaundered proceeds—e.g., acquisition of the property of enterprises, acquisition of limited corporations and co-mingling of funds through stock markets.

b) More-traditional crimes are converging with economic crime

Recognizing that many economic crimes (e.g., counterfeiting, frauds, securities manipulations, technological crimes) are, in fact, being perpetrated by organized criminals, suddenly positions offences such as fraud in a new light.

For example, Professor David Carter (School of Criminal Justice, Michigan State University) points to the convergence of four main crime trends:

- Organized crime.
- Industrial espionage.
- Violent crime.
- Computer crime.

Jack Blum (formerly Special Counsel, US Senate Committee on foreign relations, and one of the drafters of the US 1977 Foreign and Corrupt Practices Act) has identified "financial fraud" as the key threat from enterprise criminals. In his opinion, the most important enterprise crimes in the future will be international financial fraud, commercial fraud, money laundering and tax evasion. Examples of these crimes include manipulation of markets for stocks and commodities, schemes that offer investment and insurance policies that have no substance and schemes to create fraudulent commercial paper. Specific cases cited by Blum (1997) are the Nigerian letter promising huge sums of money for access to bank accounts and the manipulation of the world copper futures market.

Blum observes that government reports and police statistics lag about three years behind the new trends that are actually occurring today. He claims that when the cases that are currently in the works are completed and become "statistics", international financial fraud and organized international tax evasion will appear to dominate all criminal activity.

c) The computer is becoming an indispensable tool for committing economic crime

The computer is an essential tool for criminal groups for the very same reasons that it is useful to legitimate businesses—it facilitates faster, more productive work at lower cost, with fewer personnel. When it comes to law enforcement, new technologies are a "double-edged sword". On one hand, state-of-the-art tools (e.g., 128 bit encryption) are felt to enhance significantly the security of data transmission across computer networks. On the other hand, use of encryption codes make it more and more difficult for the police to trace and apprehend white collar criminals who use advanced techniques to hide or cover their tracks. This dilemma opens up the debate over the perceived conflict between confidentiality and public safety—an issue that may well lead to dissimilar national policies governing encryption around the globe.

This complex spiral of new and interrelated technologies is taking economic crime (as well as many traditional crimes) to an entirely new level of complexity and is calling for additional know-how on the part of investigators. The key trends and issues associated with "tech crime" are further explored in the second part of this chapter.

d) Economic crimes are transcending both geographic and jurisdictional boundaries

Local, regional and international jurisdictional issues pose very real difficulties for police investigators. The mechanisms in place today for facilitating joint investigations that cut across jurisdictional boundaries are considered to be inadequate for dealing with transborder crimes (both internationally and within Canada). White collar criminals recognize this weakness and are taking advantage of jurisdictional loopholes to minimize their risk of arrest or subsequent conviction.

Many criminals are free to move across borders, whereas law enforcement officers are hindered by restrictions related to sovereignty rights, differences in laws or their interpretation and, often-times, a lack of will or resources. As Peter Csonka, (1997, p.3) points out:

> *"criminal law enforcement systems are very much linked to national sovereignty: as soon as the policeman, the prosecutor or the judge purport to exercise their powers beyond a national frontier, they are bound to collide with the neighbour's sovereignty."*

These hurdles can have a definite detrimental impact on the successful and timely completion of economic crime investigations.

For example, on the international front, the Mutual Legal Assistance Treaty mechanism is considered cumbersome, in that it requires a lengthy process of negotiation prior to signing and the treaties vary from country to country.

> *"What is often at stake is both time and exposure of your case. Each step in these international agreements can consume months--during which time informants might be put at risk, witnesses may vanish and the case may be lost."* (Interviewed respondent for this project, Feb/98)

Furthermore, treaties are often restricted in terms of the number and kind of offences that are covered and the kind of assistance that will be given. Similarly, extradition treaties must be in place before suspects can be transported over borders.

Within Canada, confusion often arises in areas such as federal versus provincial or local investigation of economic crimes. Cases considered a high priority for the federal government, for example, may have a lower priority for the provinces (who may choose not to prosecute). This situation is made more complex by jurisdictional splits within the RCMP due to its various "contracted" roles as the provincial and municipal police force, and also between the federal RCMP role and that of other provincial and municipal police forces.

Economic crimes, by their very nature, are multi-faceted. leaving the question of jurisdiction and enforcement responsibility open to interpretation. For example, the act of passing counterfeit money or credit cards at a local restaurant in downtown Toronto could, at first glance, be considered a local, provincial or a national crime—especially if it is suspected that the perpetrator is tied to other local criminal acts. In such a situation, the law states clearly that the police of local jurisdiction retain the legal authority to initiate the investigation. However, a local police agency—particularly if it considers its own caseload to be over-burdened—may choose to draw attention to the interjurisdictional characteristics of the crime (e.g., "national interest test") in order to pass the case along to a provincial police force or, ultimately, the RCMP.

2. Reduced fiscal resources are forcing policing programs to realign the level and type of services they provide

a) The period of steady growth in police funding has come to an end

In traditional reviews of policing in Canada (and in most western countries), one trend that has remained relatively constant has been the growth of policing each year. Budgets tended to keep pace with this increase in size.

This policing "tradition" is no longer true. The costs associated with law enforcement have become increasingly debated as fiscal restraint descends upon even the policing institution. Until the early 1990s, for example, there was a consistent annual increase in the police budget. In 1990, in current dollars, there was an exceptionally high increase of 12%. By 1995, however, this increase had shrunk to 0.4% (in current dollars), which translated in constant dollars to a reduction of 1.7%.

The trend toward decreasing fiscal resources has become a harsh reality that must now be understood and accounted for in future planning of policing programs.

b) Police forces are being called upon to justify resource allocations for both existing and new programs

The resource allocation problem extends well beyond developing a compelling "business case" to secure additional funds. Requirements by external stakeholders (refer also to Section D, below) to justify not only requests for new funds, but also to preserve existing funding allocations brings into question quasi-philosophical issues regarding "what is the optimal size and resource mix required to sustain the effective operations of any police force or unit?"

Underlying the arguments surrounding this question is the notion that adequate resourcing of police operations is today, more than ever, an issue of balancing required knowledge and skills with sheer numbers of officers. David Bayley, based on his extensive international study of police forces and his intimate knowledge of police research findings, has observed that:

"Police budgeting represents the triumph of organizational process over rational decision-making. Police allocations are so constrained by customary rules and understandings that they cannot be easily shifted to more productive uses. Police management is not ends-oriented. Managers customarily fit

problems to the organization, not the organization to problems. This is why the Audit Commission (UK Audit Commission, 1991) concludes: 'The terms of public debate need to move off the assumption that more police officers and more police expenditure leads to a commensurate increase in the quantity and quality of police outputs' ." (Bayley, 1993, p.7).

Bayley argues that city and government officials, forced by restraint to try to make some sense of a relatively new value-for-money / bottom-line approach to criminal justice, must be clear of what is being offered to the taxpayer. Dollars must be tied to an evaluation procedure that can illustrate the gains "purchased" by the budgets—and, particularly, by any changes to the budget. More police resources do not automatically imply better enforcement. Instead, the kinds of resources and how they are used, supported and rewarded must also be weighed in future budgetary allocation decisions.

c) Some police services are being curtailed

Over the past decade or so, police in Canada had begun to experiment with a wide range of measures designed to reduce costs while maintaining, or even increasing, efficiency—e.g., "achieving more with less". Nowadays, in light of continued fiscal restraint, this objective has changed. Today's watchword is no longer "working more efficiently" or "doing more with less", but rather "doing less with less".

It has now become evident that some of the functions traditionally performed by police may themselves need to change in order to achieve the stated priorities of the police organization. The practice of saying "no" to taking on certain activities first surfaced in the late 1970s, but has become much more prevalent in the latter half of the 1990s.

The unrelenting pressure of decreasing resources has forced units across the policing community to question their respective mandates and to develop (or interpret policies and procedures) in such a manner that the boundaries of response are narrowed. A close-to-home illustration of this practice is the recent Economic Crime Program Mandate Study (RCMP 1998). This "mandate" (contained in Appendix B) has been presented to the Branch as a "directional statement" only, until such time as a corresponding level in resources has been determined.

3. Funding bodies are becoming increasingly involved in setting policies and priorities for law enforcement agencies

As Canada's fiscal situation deteriorated during the 1990s, governments and other funding agencies have taken a "bottom-line" approach to many forms of spending. The viability of programs has been tied to notions of "value-for-money" and "bangfor-the-buck". Resource levels for police services have been increasingly linked to performance evaluations vis-à-vis stated policing priorities.

Exhibit II-1 identifies a number of generic categories according to which operational "gains" derived from the police activities have been evaluated in certain jurisdictions (Bayley 1993, p.15).

This list is not intended to demonstrate an "ideal" set of performance indicators for evaluating law enforcement services. Instead, it is intended to illustrate the myriad of yardsticks according to which the calibre of policing could be judged.

Exhibit II-1
Sample performance measures used in policing

DIRECT

Hard

- Crime rates
- Criminal victimizations
- Ability of the public to undertake routine activities
- Real estate values
- Commercial activity in places of public accommodation
- Number of disorder situations interrupted
- Number of community "problems" solved
- Information volunteered to the police about crimes

Soft

- Fear of crime
- Confidence in the police
- Commitment to neighbourhoods
- Satisfaction with police action
- Complaints about police service
- Willingness to assist the police
- Community solidarity

INDIRECT

- Numbers of police officers
- Numbers of uniformed officers on the street
- Proportion of detectives to uniformed officers
- Ratio of supervisors to police officers
- Response time
- Arrests
- Clear-up rates
- Number of community crime prevention meetings
- Number of Neighbourhood Watch groups
- Speed in answering telephones

(Source: D. Bayley, "Back from Wonderland, or Toward the Rational Use of Police Resources, in Thinking About Police Resources, edited by Tony Doob, P. 15.)

In reflecting on the usage of performance measurement in policing agencies, Bayley cautions that an important paradoxical situation may arise. As the police become increasingly pressured to account for resources, they will tend to focus on those things that are easiest to measure—typically the indirect measures.

Traditional methods of evaluation are slowly changing as community policing gains prominence; however, when budgets are tight, sensational seizure statistics or large numbers of arrests still tend to take a priority position. Gradually, with an emphasis on outcomes, the desired "impact" may ultimately reflect the priorities of the local and national communities they serve. Under such a scenario, statistics on arrests, seizures, etc. will no longer be adequate for pleasing an increasingly aware and sophisticated public.

The RCMP, for its part, has made a foray into organization wide performance measurement in establishing performance indicators in its *Report on Plans and Priorities 1997/1998 - 1999/2000*—a successor to the annual *Part III Estimates* document required by Treasury Board. Measuring performance effectiveness in areas of economic crime such as serious frauds, computer and technological crimes and securities criminality can prove challenging, given that cases can be long and complex with "successes" hard to quantify. Furthermore, directly linking these police activities to desired "outcomes/results" for society is an even greater challenge (especially considering that outcomes such as lower crime rates are often influenced by concurrent crime prevention activities such as public/corporate awareness and education initiatives). Nonetheless, a preliminary set of expected results and performance measures associated with the RCMP's Economic Crime Program has been established. A partial list (taken from the report cited above) is presented in Exhibit II-2:

Exhibit II-2
Performance Indicators for the Federal Policing Services at the RCMP

Results Expected	Performance Measures
To reduce the economic incentive for enterprise crime	Increases in the value of assets/seizures under the Integrated Proceeds of Crime, Proceeds of Crime and Anti-Smuggling Initiative, including monies, property, all types of vehicles, drugs and contraband goods
To reduce opportunities for transborder crime	Decreases in organized illegal entries into Canada, alien smuggling organizations, suppliers of forged travel documents and counterfeiters of currency and negotiable instruments
To improve the police response to organized crime	Number of successfully completed organized crime investigations resulting in prosecutions
To contribute to a reduction in economic crime	Increases in successful investigations and arrests for white collar crime in areas such as corporate crime, corruption, telemarketing fraud, securities and stock market fraud

N.B. These performance indicators are not the exclusive responsibility of the Economic Crime Program, but rather are shared across various programs which fall under the umbrella of Federal Policing Services.

This inter-related nature of the performance measures underlines the degree to which economic crimes are converging with other forms of organized crime, thereby complicating the task of attributing benefits associated with "economic crime" (as distinct from other forms of crime). Furthermore, while stated performance indicators focus on the *number* of successful prosecutions, some people question the value of such measures, suggesting instead that the simple fact that there are well publicized prosecutions and convictions should suffice to reinforce the desired deterrent effect for the vast majority of the population and to preserve the integrity of Canada's business and financial services in the public eye.

4. Police forces are losing their traditional "monopoly" over policing services

a) Private agencies are offering security and investigative services that were once the exclusive domain of public police forces

Years ago, "policing" was understood to mean "public policing". Today, however, the points along the policing spectrum are becoming increasingly blurred. For example, public policing services provided at the national, provincial and local level, are supplemented by enforcement officers (e.g., park wardens and customs officers) working on behalf of government agencies. Privately funded protection and investigation services also serve to protect both the interests of the general public, companies and individuals. Investigations of economic crime are frequently pursued by representatives of securities commissions or by third-party forensic accounting firms.

The 1971 Rand Report (Kakalik and Wildhorn) in the US, and research by Philip Stenning and Clifford Shearing during the late 1970s and 1980s, have pointed to a gradual increase in interest in private security. The diversity of investigative and other policing services now carried out by both private and publicly funded operations includes:

- Patrol/detective work.
- Emergency response.
- Frauds (domestic and international).
- Corporate and residential security.
- Special investigations (homicide, rape, arson, money laundering, etc.).

What has become apparent is that public police forces can no longer, by themselves, meet the policing and security needs of the population. Accomplishing this ever-broadening range of tasks has meant that reliance must increasingly be placed on partnerships across the various policing agencies.

Discussions used to focus on the blurring between private and public "space". This discussion may be largely irrelevant today since both "spaces" are policed by an array of groups offering (similar or complementary) policing services.

Re-thinking the make-up and the measures of success for the police are not the sole positive outcomes of restraint. Following the adage of "necessity being the mother of invention", police forces are having to work in partnerships in ways previously unheard of—not merely in joint force operations with other police departments, but also with other agencies. The police now work with securities commissions, banks, and corporations, in addition to an array of community groups as a result of community policing. A recent example from the RCMP document *Report on Plans and Priorities 1997/1998 - 1999/2000* (p. 15) is the consortium that developed the MICA software—including RCMP, stock exchanges, securities commissions and investment dealers associations.

These joint-operations and partnerships go beyond the simple sharing of resources. Once "teething problems" associated with any new joint venture are overcome, a variety of other advantages can be found, including:

- Cross pollination of methodologies and attitudes of the different agencies.
- Shifts in inbred agency cultures.
- Ability to make use of the different technical resources and legislative powers of each agency.

b) The mandate and priorities accorded to public and private policing agencies often differ

While the value of encouraging integration between the various forms of policing has been presented, several important differences should also be acknowledged. For example, police forces representing the state may work on a given case with the objective of laying formal criminal charges. By contrast, a company may hire private investigative services to ensure the corporation ceases to be victimized (e.g., placing "reimbursement for losses incurred" ahead of "ensuring due justice is served").

The following issues will become increasingly pertinent as the private "policing" (e.g., protection and investigation) industry grows:

- Invisibility of both offences and sanctions within the "private" sphere.

- Foreign ownership of private policing firms.

- Unequal distribution of "policing" to those willing to pay (e.g., investigation of those crimes for which there is a "paying customer").

- Sharing of confidential information between private and public investigators.

- Implications for the Charter of Rights as cases are diverted from the formal justice system (Trofymowych, 1993).

The opportunity for the private sector to provide increasing levels of protection and investigative services once perceived to be the exclusive domain of public police agencies carries with it the question of "who should pay" and "whose interests are being served". These issues are particularly important in the realm of both economic and technological crime, where a high proportion of crimes against private companies are, in fact, committed by those companies' own employees. The circumstances under which the RCMP (or other public police agency) should investigate such crimes—at public expense—remain unclear:

- Should public money be spent to address vulnerabilities to fraud that result from a corporation's unwillingness to put in place adequate governance and control mechanisms?

- Should the RCMP focus instead on the prevention of corporate crimes through education and awareness campaigns, conducting investigations only for high dollar value or organized crimes? (And if so, is justice ever fully served to white collar criminals?)

5. Increased demands to account for police actions have added to the workload of investigators

Trends identified above have introduced the notion of increased fiscal accountability and methods that governments, police boards and police management are using to monitor inputs and outcomes of police activities. A second form of accountability relates to use of police powers and accountability for procedures.

A number of Supreme Court and Charter decisions have profoundly impacted on how the police must carry out policing activities. Cases such as R v Stinchcombe (1991) have been interpreted to have far reaching effects on the police in the area of "disclosure". For example, investigators must budget for additional cost and time to duplicate all notebooks, witness materials and other key documents so that they be made available to the defence team. Furthermore, cases such as R v Duarte (1990), R v Wong (1990) and R v Wise (1992), caused delays to investigations while surveillance legislation was updated, clarified and amended. The often overburdened judicial process itself can also be onerous. This additional administrative burden reduces the proportion of time officers are able to spend conducting the investigation itself.

A further layer of scrutiny is placed on police investigators by the media who keep an open eye for Charter violations or other weaknesses in police procedures. Police awareness that they must maintain meticulous respect for procedures when conducting investigations has been further heightened during the past year by high profile cases in the Canadian and international media.

6. The international community is pressuring countries to "pull their own weight" in the development and enforcement of economic crime laws

Policing today is truly a global concern. Any country will become a haven for white collar criminals to the extent that its laws are deemed to be weak or incomplete or if officials are viewed as corrupt or inadequate. As a result, more than ever before, there exists a strong pull in the international community toward the harmonization of laws and the coordination of policing strategies. The pressure felt by Canada to adhere to international standards is heightened by the country's proximity and similarity to its powerful neighbour to the south.

In recent years, Canada has taken a strong role in many such international agreements. Canada has been an active member on groups such as the Financial Action Task Force (FATF) and the Inter-American Drug Abuse Commission (CICAD), as well as an observer on a number of working groups dedicated to promoting the uniformity of laws and increased sharing across jurisdictional boundaries.

The enforcement of these new agreements, once passed into law, typically becomes the responsibility of national policing agencies. Examples of legislation currently being drafted include Canadian legislation governing suspicious transaction reporting and centralized reporting of high value crossborder cash flows (Source: Solicitor General, *Annual Statement On Organized Crime*, Nov. 1997). These pieces of legislation are intended to provide police and customs officers with the necessary tools "to target more forms of criminal profiteering".

A companion piece, purported to be in the works, is the founding of a financial intelligence unit to collect and analyze this "new" information. All of these changes—regardless of how desirable—have a significant impact on the RCMP (and perhaps more specifically on the Economic Crime Branch and the Proceeds of Crime Branch).

7. The public perceives economic crime as a lower priority than physical/violent crime

a) Economic crime is not well understood by the public

Criminology literature going back to the classic 1945 work of Edwin Sutherland has tried to understand why the public refuses to regard economic crime as a serious threat (see also Levi 1987 and 1985, and Stanley 1996).

Despite the increasing links between economic crime and organized crime, a major difficulty for the police community remains sensitizing the public and political funding bodies, and even the criminal justice system, to the seriousness of economic crime. A number of factors have been cited as contributing to lack of public attention relative to other forms of crime that economic crimes have drawn.

For example, whereas people can easily identify with victims of physical violence or theft of personal property, a common perception is that economic crimes are "victimless crimes". Little sympathy is offered to institutions or corporations that fall victim to white collar crime, since many view them as impersonal entities having "endless resources" or compensatory insurance coverage. By contrast, the losses of individuals who fall prey to scam artists are often portrayed in the media as resulting from the victim's own imprudence or greed.

Another prime reason for the lack of public awareness is the sheer complexity of economic crime cases. Apart from a handful of highly sensational cases (e.g., financial collapses or scandals) that are fueled through the media, the multitude of routine cases can often be so complex that investigators and juries—let alone the average public—cannot readily understand what has actually taken place.

Even the terminology that is commonly used to describe economic crime (e.g., white collar crime, business crime, financial crime, regulatory offence, etc.) contributes to toning down the seriousness of the violation.

Finally, large "serious" frauds are not uncovered on a daily basis. They tend to remain hidden, often well orchestrated conspiracies, set up to operate over the long term and facilitated by various forms of corruption.

b) Many economic crimes go unreported to police agencies and are not reflected in crime statistics

The tally of economic crime statistics reported by police agencies reflects only part of the overall economic crime story. Attempting to obtain a more complete picture of the level of economic crime in the country requires, at minimum, cross-referencing reported police statistics with the findings from surveys of victims. As one might typically expect, the larger the case, the greater the tendency to report the crime. However, the more sophisticated the criminal operation, the less likely it will be detected.

In relatively minor fraud cases there may be a sense by the public that the police will not be able (or willing) to solve the case. However, even when very large financial frauds are detected, there are often compelling reasons for organizations to keep such information away from the public (and hence away from the public police). There are a number of reasons for this:

- In certain fraud cases, exposure to the general public of the methods used by criminals may be either detrimental or embarrassing to a private company, securities commission or financial institution. Many organizations fear negative publicity or would worry that competitors might use this information to their advantage. Many private companies have established their own internal investigative units and report crimes only once they have identified an individual to prosecute.

- In significant financial fraud cases, the "victim" (e.g., private or public institution) will tend to focus first and foremost on ensuring the fraud ceases immediately. Lengthy time frames that are often necessary when public police take on a specific case, often compels the organization to refer instead to a private police services agency, such as a forensic investigative firm. Such cases frequently do not make their way into police statistics, unless resolution of the case requires recourse to the formal criminal justice system.

Lack of awareness and concern over economic crime might also be a reflection of the "spin" that the media give an economic crime story. For example, an article on fraud statistics published by Statistics Canada (Globe and Mail, February 25, 1997) announces in its headline that the "fraud rate drops to lowest level in 20 years". Upon closer reading, one realizes that, in fact, the sharp drop in "cheque fraud" (caused presumably by plummeting cheque usage in Canada) overshadows a sharp increase in credit card scams and automated teller machine thefts.

As the 1998 report *Fraud in Canada 1977-1996* (recently released by Statistics Canada) states:

> *"Patterns in various fraud offences over the past 20 years can be attributed to several factors such as the reporting practices of victims, changes in police operations, reporting practices of businesses and/or*

corporations, increased use of private security agencies, difficulties in detecting newer types of fraud and an overall change in consumer behaviours."

B. Technology related trends and issues

Six major technology trends have been identified:

- Computers have permeated virtually all aspects of Canadian society and have become thoroughly entrenched in the workplace.
- New technologies are proving to be powerful tools for facilitating traditional crimes and for committing new forms of crime.
- Transnational, organized criminals are harnessing technology to facilitate activities in a range of areas such as gambling, drug trafficking, prostitution, smuggling, etc.
- Criminal adaptation of leading edge technology is evolving as quickly as new technologies are being introduced.
- Police forces around the world have been unable to keep up with the rapid growth of technology and its use in crime.
- The electronic information infrastructure which supports every sector of the Canadian economy—from financial services to government to health care—is vulnerable to sabotage.

1. Computers have permeated virtually all aspects of Canadian society and have become thoroughly entrenched in the workplace

Over the past 15-20 years, the computer has become a day-to-day "workhorse" within most office environments in Canada. In recent years, breakthroughs in terms of processing speed, memory capacity, miniaturization and networking have fueled spin-off technologies, which have come to influence virtually all aspects of life.

Whether purchasing theatre tickets from a vending machine or conducting personal banking by telephone, the use of computers to handle everyday transactions has become commonplace. Information in all forms has become a portable resource that can be readily shared through interlinked computer networks (or via ordinary telephone lines). Similarly, billions of dollars in electronic funds can be shifted around the globe at the press of a button. The Internet has provided a "virtual frontier" that puts a global knowledge base at everyone's fingertips, furthering the expansion of computers into both school and home life.

Exhibit II-3 provides a series of examples to demonstrate that the current trends in computer growth are showing no signs of abating.

The "sky-is-the-limit" potential for technology advancement has been further assisted by simultaneous pressures to globalize business and financial dealings, harmonize regulations/standards and eliminate barriers to trade (e.g., through regional associations and trading blocs).

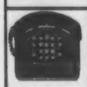
2. New technologies are proving to be powerful tools for facilitating traditional crimes

While new information technologies, including the Internet, provide police investigation teams with new instruments to conduct their research, such tools can equally be used to carry out criminal activities such fraud, embezzlement, as well as other non-economic crimes. In fact, the February 1998 UK Audit Commission report predicts that the Internet could turn out to be the "**security challenge of the millennium**".

For example, the Internet provides a global forum for the instantaneous cross-border transfer of illicit funds and the distribution of information ranging from stolen credit card information to passwords / access codes and pirated software. Other Internet activities can also prove lucrative to criminal elements: pyramid programs, chain letters, telemarketing scams targeting the elderly, stock market manipulation, etc.

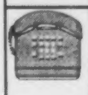
Law enforcement agencies have identified that new technologies are being used in carrying out two broad classes of illegal activity: 1) "computer-assisted crime" (whereby traditional crimes are facilitated by using computer technology); and 2) "computer crime" (wherein computers or their contents are the target of the offence). The line between the two is blurred and the skills required to investigate computer crimes and computer-assisted crimes often overlap and vary on a case-by-case basis. While "computer crime" invariably calls for a high degree of specialized knowledge (e.g., encryption techniques), a similar skill profile might also be called for on a "computer-assisted crime" case. (More and more, computer skills are being called for to facilitate investigations across many areas of policing.)

Exhibit II-3
Rate of technological evolution—examples

	5 Years Ago	Today	5 Years From Now
	• *Limited* use of dedicated lines for electronic commerce between businesses. • Information exchange via the Internet *predominantly* for R&D and academic/military purposes.	• *Limited* use of the Internet for electronic commerce (e.g., sale of goods and services). • Information exchange via the Internet available for a *small* part of the Canadian population.	• *Widespread* use of electronic commerce between businesses and consumers over the Internet. • Information exchange via Internet readily available to a *majority* of the Canadian population.
	• *Predominantly voice* transmissions. • Transmissions *relatively easy to intercept.* • Encryption technology *limited* to government, military, bank and insurance transactions.	• *Equal voice/data* transmission levels. • Some computer/network expertise required to intercept. • Encryption technology *standard* for Web browsers.	• *Predominately data* transmission. • Significant *expertise required to intercept.* • Secure digital networks and *widespread* use of encryption for all transactions (supplemented by the use of digital "certificates").
	• *Decentralized* control over networked PC's.	• *Mix of central and decentralized* control of administration and security over networked PC's.	• *Centralized* control over administration and security of networked PC's.
	• *Limited* use of colour copiers.	• *Widespread* use of low resolution colour printers and color copiers. • *Limited* use of color laser printers.	• Photo realistic printing *widely* available.
	• Discount brokerage firms introduce PC banking. • Debit cards introduced.	• *Limited* Internet banking and trading through discount brokerages. • *Widespread* use of debit cards. • Smart Cards introduced for payments with new security features.	• *Widespread* Internet banking and trading through discount brokerages on stock markets around the world. • *Widespread* use of Smart Cards with embedded systems to control access to transactions.

Sources:
Fortune: Mr. Gates builds his Brain trust, pp.84, December 1997
Wired: New Rules for the New Economy, pp.140, September 1997
The Economist: Doubling Games, A Connected World, Better Faster Cheaper, From Circuits to Packets, www.economist.com
The Economist: Death of Distance, 30th September, 1995
Morgan Stanley Dean Witter: Technology Internet/New Media, 23.September, 1997
Morgan Stanley: Internet Retail, 28. May, 1997
Information Society Initiative: Moving to the Information Society, United Kingdom, 1997
Sun Microsystem: www.sunmicrosystem.com, March 1998

Exhibit II-3
Rate of technological evolution—examples

	5 Years Ago	Today	5 Years From Now
	Limited use of dedicated lines for electronic commerce between businesses.	*Limited* use of the Internet for electronic commerce (e.g., sale of goods and services).	*Widespread* use of electronic commerce between businesses and consumers over the Internet.
	Information exchange via the Internet *predominantly* for R&D and academic/military purposes.	Information exchange via the Internet available for a *small* part of the Canadian population.	Information exchange via Internet readily available to a *majority* of the Canadian population.
	*Predominantly voice* transmissions.	*Equal voice/data* transmission levels.	*Predominately data* transmission.
	Transmissions *relatively easy to intercept.*	Some computer/network expertise required to intercept.	Significant *expertise required to intercept.*
	Encryption technology *limited* to government, military, bank and insurance transactions.	Encryption technology *standard* for Web browsers.	Secure digital networks and *widespread* use of encryption for all transactions (supplemented by the use of digital "certificates").
	Decentralized control over networked PC's.	*Mix of central and decentralized* control of administration and security over networked PC's.	*Centralized* control over administration and security of networked PC's.
	Limited use of colour copiers.	*Widespread* use of low resolution colour printers and color copiers. *Limited* use of color laser printers.	Photo realistic printing *widely* available.
	Discount brokerage firms introduce PC banking.	*Limited* Internet banking and trading through discount brokerages.	*Widespread* Internet banking and trading through discount brokerages on stock markets around the world.
	Debit cards introduced.	*Widespread* use of debit cards. Smart Cards introduced for payments with new security features.	*Widespread* use of Smart Cards with embedded systems to control access to transactions.

Sources:
Fortune: Mr. Gates builds his Brain trust, pp.84, December 1997
Wired: New Rules for the New Economy, pp.140, September 1997
The Economist: Doubling Games, A Connected World, Better Faster Cheaper, From Circuits to Packets, www.economist.com
The Economist: Death of Distance, 30th September, 1995
Morgan Stanley Dean Witter: Technology Internet/New Media, 23.September, 1997
Morgan Stanley: Internet Retail, 28. May, 1997
Information Society Initiative: Moving to the Information Society, United Kingdom, 1997
Sun Microsystem: www.sunmicrosystem.com, March 1998

3. Transnational, organized criminals are harnessing technology to facilitate activities in a range of areas such as gambling, drug trafficking, prostitution, smuggling, etc.[2]

One of the alarming trends in technological crime has been the increased adoption of new technology by organized crime groups in conducting criminal activities. For example, state-of-the-art technologies have led to a shift away from traditional "basement counterfeiting operations" to sophisticated mass production of forged currency, cheques, transaction cards and bank drafts by international rings who have recognized its high profit potential. Technology also enables these traditional criminals to expand and strengthen their existing activities by weaving in white collar crimes such as money laundering and tax evasion.

David Carter (1997) identifies a number of the more common uses of computers in conducting organized crime operations:

- Contraband shipment schedules.
- Income and expenses of contraband or commodities.
- Data bases of conspirators or customers.
- Locations, account numbers and status of monetary transactions.
- Monetary transfers and payments.
- Status of bribed or vulnerable officials.
- Dossiers of officials, conspirators, and others of interest to the crime group.
- Direct criminal activity such as counterfeiting (including certificates of ownership), scanning, graphics.
- Pornography industry: production / distribution / transmission of photos and written materials; advertising, sales and appointments with prostitutes (e.g., "cyber-brothels").

---

[3] *Source: Transnational Crime and Policing: An RCMP Perspective by Insp. T. G. Killam—Presentation to the Conference on Management Challenges in 21st Century Policing, Ottawa, Sept. 22-24, 1995.*

4. Criminal adaptation of leading edge technology is evolving as quickly as new technologies are being introduced

The technological skills of criminals are widely acknowledged. However, the response to date by law enforcement to this type of criminal activity has not always been adequate. Just as the financial sector introduces new procedures or devices to negate the actions of white collar criminals, new methods are devised to bypass these regulatory/enforcement efforts (e.g., DirecTV and digital telephones).

For example, the banking community speaks of the "costs of doing business" whereby a certain amount of both internal and external fraud is tolerated (if not expected). When this level extends beyond a preset limit, the bank is forced to change the technology that is being violated. Depending on the nature of the fraudulent activity, the banking community may have internal technological experts who can monitor and detect the weaknesses in prevailing systems and hence are able to introduce new products. Law enforcement can seldom respond as quickly.

Indeed, many believe that today's requirements in law enforcement can only be met through a public/private sharing of expertise and resources. For example, Grabosky and Smith (1997), in referring to telecommunications related illegality, predict that increasingly the solution to high-tech offences will be a mix of law enforcement, technological and market solutions.

It should be noted, however, that the magnitude of effort and resources required to provide an effective, sustainable response to the problem of technological crime is, at best, difficult to ascertain. Gauging these requirements will necessitate looking beyond the hype associated with a number of well publicized and sensational cases to the more fundamental issues of "actual economic crime" and "potential for crime".

> *"...much telecommunications related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control... security in cyberspace will depend on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of cyber-crime".*
> (Grabosky and Smith, 1997, p.6)

Grabosky cautions that the technological abilities of criminals can be exaggerated—either by the criminals themselves, by law enforcement or by academics—each for different reasons:

Many people, regardless of their calling, are inclined to accentuate their accomplishments. Telecommunications criminals are no exception. While some thrive on anonymity, others seek notoriety. This latter group often embroider their activities. There is a significant gap between what they do, what they say they do *and what they think they do. Law enforcement agencies, on the other hand, have been known to overstate the magnitude of a problem in order to justify maintaining or enhancing their resource base. Other actors who arguably have commercial incentives to accentuate the gravity of a problem include the security industry and the news media. (Grabosky and Smith, 1997, p.15).*

At a minimum, the interviews and research conducted as part of this study all tend to corroborate that the threat posed by "tech crime" is as great as (if not significantly greater than) the actual occurrences to date.

Regardless of the magnitude of economic crime, or its potential threat, what is clear is that addressing the challenges and complexity of white collar crime will require an as-yet-to-be-determined balance of business/computer skills and traditional investigative know-how. Today's resource estimates will no doubt need to be revisited in the future as the scope and magnitude of the impacts of "tech crime" become clearer.

5. Police forces around the world have been unable to keep up with the rapid growth of technology and its use in crime

As new technology continues to expand into all walks of life, more and more opportunities will undoubtedly arise for individuals and organizations to use technology in committing virtually every kind of crime. Advanced telecommunications and computer technologies have converged and become intertwined, opening the door for countless new applications of technology in committing criminal acts.

> *"The internationalization of money markets and the commercial and business infrastructure in general means that even the most straightforward of frauds may now involve institutions which are based in a foreign country either as victim or as unwitting providers of services to fraudsters*".
> (UK, Chief Constable C. Phillips, 1997, p.7)

All major western countries have defined technological crime as being a high priority. Canada is no exception. Canadian political officials and ministers have signed conventions, taken part on international task forces, and have urged, in diverse ways, countries around the globe to act with some degree of uniformity on criminal matters that affect all other countries.

For example, at the December 1997 Summit of the Eight in Denver, a group of ministers from the "G8" countries met and pledged cooperation to fight computer crime, with an emphasis on "cyber-crime" and high-tech crimes.

"As a group, we recognize that we have entered a new age- the computer age. Twenty-first century technologies are going to change how we live and make many things easier. But computers and networks are also opening up a frontier of crime. Criminals no longer are restricted by national boundaries". (US Attorney General, Janet Reno in a speech at FBI Headquarters, December 11, 1997)

Under the agreement, **Canada**, France, Germany, Japan, Italy, Russia, the UK and the US committed to the following:

- Increase training for law enforcement fighting technical computer crime.
- Ensure sufficient numbers of law enforcement personnel allocated to combat high-tech crimes.
- Establish a 24 hour hot-line for crises requiring assistance beyond domestic capabilities.
- Develop new technologies to allow for faster tracing of network intruders back to the source of the attack.
- Increase cooperation on crimes where extradition is not possible because of nationality.
- Encourage greater archiving of information at network choke points so that information crucial to prosecutions will more likely be retained.
- Work with industry on new anti-crime technologies.
- Review legal systems to ensure they appropriately criminalize abuses of telecommunications and computer systems.
- Consider issues of high-tech crimes where relevant when negotiating mutual assistance agreements or treaties (MLATs).
- Ensure that MLATs allow for high speed transmittal of information (by e-mail, fax etc.) in cases involving high-tech offences.

For the time being, these statements represent largely a set of symbolic principles toward which the signatory countries have agreed to work. The path forward to implementation, however, remains unclear.

In Canada, for example, the federal government has announced that its national response initiatives would be spearheaded by the RCMP, however, no additional resources have been allocated to date to fund this endeavour. To date, Canada's governments have maintained their steadfast focus on fiscal/budgetary restraint forcing the RCMP, in fact, to postpone any significant new investment in related people, training and equipment upgrades. These factors have hampered the

RCMP's ability to mount a concerted campaign to counter the threats brought to bear by technological crime in Canada.

By contrast, the US Federal Bureau of Investigation has responded to the growing number of instances in which criminals have targeted major components of information and economic infrastructure systems by establishing International Computer Crime Squads in selected American cities. These squads have been mandated to investigate intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes where the computer is a major factor in committing the criminal offence.

> *"Today when new FBI agents graduate from our training academy... they leave with their firearms and their badges, but they also leave with a laptop computer... It is imperative for the way they must conduct investigations. When they serve law enforcement search warrants, they seize hard drives and disks instead of the boxes and boxes of records and books and ledgers that their predecessors, myself included, used to seize to support our cases"* (Louis J. Freeh, Director of the FBI, in a speech at an International Computer Crime Conference in New York on March 4, 1997).

One fact that has become clear to the signatories of the December 1997 declaration is that the chain of protection against high-tech crime will only be as strong as its weakest link. As with all other crimes that reflect the global economy, all countries are at the mercy of those countries whose regulation, enforcement and know-how lag behind. Similar to money laundering offences, criminals will seek out the country showing the most cracks in the system as the home base or conduit for their criminal activity. Canada and Canadian law enforcement therefore face a responsibility not only to Canadians, but also to international partners who are pressuring Canada to become more proactive in preventing, deterring and responding effectively to high-tech criminal activities.

Building a coherent and effective international response to this challenge is further complicated by the increasing complexity of national and international law from a criminal investigative and prosecution viewpoint. Complex webs of geographic and territorial (e.g., mandated) law enforcement boundaries have no bearing on organized criminals employing new computer technologies, but instead impede police in conducting their investigations. These technologies permit internationally organized criminals to circumvent traditional border enforcement mechanisms with ease, rendering near meaningless such traditional law enforcement "tools" as search warrants and traditional electronic surveillance mechanisms. In addition, crime prevention strategies (e.g., "suspicious conduct" and "know your client" policy guidelines recommended for financial institutions) become outmoded in the absence of face to face client contact with clients.

6. The electronic information infrastructure which supports every sector of the Canadian economy—from financial services to government to health care—is vulnerable to sabotage

Our national critical infrastructures—energy, banking and finance, telecommunications, transportation and government/emergency services—must be viewed in the context of the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence.

Major infrastructure categories include banking/finance, telecommunications, transportation, as well as government and emergency services.

This interlinkage has created a new dimension of vulnerability, which combined with an emerging constellation of threats, poses unprecedented national risk.[3]

> *"Because of industry and government's dependence on computer systems, security of an IT system should be a top priority for anyone seeking to minimize their exposure to computer risks".* (British, Audit Commission Report, Feb. 1998 reported by Newsbytes News Network, Steven Gold)

The 20-year trend data provided in Exhibit II-4 gives evidence of the rapid rate of technological change and modern society's dependence on technology.

Exhibit II-4
Global technology trends (and projections)

Category	1982	1996	2002
Personal Computers	Thousands	400 million	500 million
Local Area Networks	Thousands	1.3 million	2.5 million
Wide Area Networks	Hundreds	Thousands	Tens of thousands
Viruses	Some	Thousands	Tens of thousands
Internet Devices Accessing the World Wide Web (WWW)	None	32 million	300 million
Population with Skills for a Cyber Attack	Thousands	17 million	19 million
Telecommunications Systems Control Software Specialists	Few	1.1 million	1.3 million

Source: "Critical Foundations: Protecting America's Infrastructures" (The Report of the President's Commission on Critical Infrastructure Protection), Washington, October 1997

---

[3] *Source: "Critical Foundations: Protecting America's Infrastructures" (The Report of the President's Commission on Critical Infrastructure Protection), Washington, October 1997, p. ix.*

The projections for the year 2002 point to a growth in the number of potential targets for a "cyber attack" evidenced not only in the burgeoning number of computer networks and Internet links, but also in the number of people possessing the technical know-how to launch such attacks. Furthermore, public telecommunications networks are becoming increasingly software driven and remotely managed through computer networks, making them vulnerable to an ever rising number of systems control software specialists who have the requisite tools and skills required to disrupt them.

"The advanced societies of today are more dependent every day on the electronic storage, retrieval, analysis and transmission of information. Defense, the police, banking, trade, transportation, scientific work and a large percentage of the government's and the private sector's transactions are on-line. That exposes enormous vital areas of national life to mischief or sabotage by any computer hacker and concerted sabotage could render a country unable to function." ("Postmodern Terrorism" by Walter Laqueur—Chairman of the International Research Council at the Center for Strategic and International Studies—in Foreign Affairs, September/October 1996).

As a supplement to the FBI's International Computer Crime Squads, US Attorney General Janet Reno recently announced the creation of the National Infrastructure Protection Centre (NIPC), a collaborative organization composed of partners representing federal agencies and private industry. The NIPC's main focus will be to serve as the government's lead mechanism for responding to an infrastructure attack.

"A recent exercise by a government agency that is responsible for maintaining and transmitting secure information... ran some computer attacks against its own very well defended systems, using people inside and outside the agency to perform them. The results of the test were that 88 percent of the attacks were successful. The implications of that exercise, translated to all our informational systems are sobering." (Louis J. Freeh, Director of the FBI, in a speech at an International Computer Crime Conference in New York on March 4, 1997)

III

Impacts Of Economic Crime

This chapter examines the magnitude and impacts of economic crime in Canada and, based on this information, considers one of the primary objectives set for this project by the RCMP: *to identify the financial and economic impacts on Canadians should RCMP resources not be able to carry out the (Economic Crime) Program's mandate (PO1).* In doing so, we:

- Present an analytical framework for describing and analyzing the magnitude and impacts of economic crime.
- Summarize estimates of the magnitude and impacts of various types of economic crimes covered by the Program.
- Summarize stakeholder views on the role and positioning of the RCMP vis-à-vis these stakeholders, paying particular attention to the issue of what would happen if the Program did not have the resources to carry out its mandate.

A. Framework for describing and analyzing the magnitude and impacts of economic crime

The previous chapter of our report reviewed external trends and issues facing the Economic Crime Program. A number of these trends are particularly significant in the way that the magnitude and impacts of economic crime are changing. These are:

1. Increasing reliance on computer and telecommunications networks as the key medium for conducting business.
2. Increasing risks of intentional disruption or damage to these systems.
3. Increasingly global nature of business and of many types of economic crimes.
4. Increasing involvement of organized crime groups in economic crimes. An associated trend is the increasing varied nature and ethnicity of organized crime groups.

5. Generally low levels of public concern over economic crime, with the exception, at present, of telemarketing fraud.

6. Increasing inter-dependence of police forces and other stakeholders to achieve optimal levels of prevention, detection and investigation of economic crimes.

7. Increasing complexity of many economic crime investigations, driven by the justice system's rules for evidence and the often complex scale of many major investigations.

8. Growing international recognition of, and support for, the need to increase policing resources devoted to economic crime; a trend that has yet to have an impact in Canada.

In order to discuss and understand the impacts of economic crime, and the way the above trends influence the impacts, it is important to have an analytical framework that, for each type of economic crime, identifies who the target victims are, characterizes the impacts of the criminal activities, characterizes the context in which the activities take place (that is, the scale of related economic sectors), and identifies major stakeholders and their roles in preventing, detecting, investigating or prosecuting these criminal activities. The key parameters for this analysis are summarized in Exhibit III-1.

B. Summary characteristics of the magnitude and impacts of economic crime

The following sections summarize the key findings from our review of published information relating to estimates of the magnitude and the impacts of each of the following types of economic crime, using the framework presented in Exhibit III-1:

- Commercial fraud.
- Securities fraud.
- Telemarketing fraud.
- Internet fraud.
- Unauthorized use of computers/mischief to data.
- Theft of telecommunications.
- Fraud related to selected Federal statutes and programs (focusing on fraud related to Employment Insurance, tax avoidance, criminal bankruptcies) and corruption or financial theft cases where the Government of Canada is the victim.
- Currency counterfeiting.
- Payment card fraud.

Exhibit III-1
Framework for analyzing economic crime impacts

Key dimensions	Potential characteristics/considerations
1. Who is targeted by the criminal activity?	• Victims may be either: – Individual consumers or investors who make payments to fraudsters. – Enabling business or public service organizations that provide the national economic infrastructure.
2. What is the estimated total financial magnitude of different types of economic crime?	• Financial magnitudes may be expressed in such terms as: – Actual losses, e.g., the value of payments to fraudsters (e.g., telemarketing fraud, securities fraud). – The value of revenues that would otherwise be received by enabling organizations (e.g., telecommunications theft). – The retail or market value of fraudulent activities (e.g., counterfeit currency, payment card fraud). – The estimated cost of disruptions to businesses (e.g., unauthorized use of computers and mischief to data). – The value of intentional non-payments, e.g., tax avoidance.
3. What is the nature and scale of related economic sectors?	• Most types of economic crime are linked to a sector, or sectors, of the economy. The nature of these sectors—growth rates, technological and economic trends—also needs to be understood, particularly in terms of identifying "where the money is".
4. What economic and social impacts do economic crime activities have?	• The consequences for Canada, and Canadians, of each type of economic crime. Potential impacts may span the range of: *For individual consumers* *For enabling business and/or public organizations* *For the economy in total.*
5. What roles can, or should, stakeholders play?	• Considerations here relate to the roles different stakeholders may play in either preventing, detecting, investigating or prosecuting economic crimes, plus potential areas of overlap and/or opportunities for improved cooperation.
6. What emerging threats or risks do stakeholders see?	• Changes that are expected to have an impact on the demand for policing or the nature and complexity of investigations.

At the outset, it must be stated that there is a dearth of official, or well-substantiated, estimates of the magnitude of economic crime. A similar situation applies to quantitative information on the economic and social impacts. Notwithstanding these data limitations, political and stakeholder concern is growing within the U.S. and Europe regarding the growing level and complexity of economic crime, and the increasing involvement of organized crime groups. Stakeholders in Canada share these concerns but political and public concern has been muted, with the possible exception of telemarketing fraud.

1. Target victims may be individual consumers or business and public organizations that provide Canada's economic infrastructure

Victims of economic crime typically fall into either of two groups:

a) Individual consumers and investors

Individual consumers and investors who are duped into making payments to fraudsters; who lose money as a result of actions by fraudsters; or, who experience disruption and inconvenience when their "financial identity" (e.g., credit card and debit card details) is stolen and must be recreated. These types of victims occur in:

- Securities fraud
- Telemarketing fraud
- Internet fraud
- Payment card fraud (primarily debit card fraud plus identity theft).

b) Private and public organizations that provide Canada's economic infrastructure

Private and public sector organizations that provide and maintain Canada's economic infrastructure. These enabling organizations become victims when they are duped into making payments to fraudsters; incur revenue losses when their services are used with no intention of making payment or when the organization assumes liability for improper use of services (e.g., with stolen credit cards); or, suffer damage or disruption to their computer and telecommunications systems from hackers. Enabling organizations are most likely to be victims of:

- Commercial fraud (which affects all business and public organizations, not just the enablers of economic activity)
- Unauthorized use of computers and/or mischief to data
- Theft of telecommunications
- Fraud and tax avoidance under federal programs and statutes
- Counterfeit currency
- Payment card fraud.

This demarcation between types of victims is very important. In situations where the victim is most likely to be an individual consumer or investor there may be no large enabling organizations with direct incentives to minimize the threat and incidence of economic crime. In other words, there's no one looking out for the interests of the "little guy".

Or, as is the case with securities fraud, the organizations concerned with maintaining fair and efficient markets are facing resource limitations and weaknesses in the national regulation of securities. In this situation, while there may be an intent to look after the "little guy", the regulatory workload may be preventing an effective response. Evidence of this issue can be found in the recent report of the Mining Standards Task Force:

> *"The Task Force does not view fraud and other financial crimes as victimless. An investor who loses his or her entire capital to a fraud is a victim of serious crime. The state that passes laws without the will or ability to enforce them adequately will sacrifice its credibility. Fraud in securities markets must be dealt with forcefully to keep it from multiplying. .....*
>
> *We recommend that:*
>
> *b) the federal and provincial governments expand the size, funding and scope of their market fraud units to a level at least sufficient to respond effectively to fraudulent activity in the securities markets, particularly in the mining sector, as well as develop strategies to attract and train investigators with the necessary mining industry, securities industry and legal expertise, and to retain that expertise so as to provide an effective ongoing enforcement program."*[4]

2. Economic magnitude of economic crime is estimated to be at least $2.1 to $3.1 billion

Our review of published information on the magnitude and scale of economic crime, and interviews with a cross-section of stakeholders, shows that the sums involved—be they losses to individual consumers and investors or to large companies and public service organizations—are substantial. Equally noteworthy is the rate at which the volume and value of economic crime appears to be growing, as indicated by trends in the value of these crimes or rates of growth in related economic sectors.

The total estimated magnitude of the selected types of economic crimes analyzed is at least $2.1 to $3.1 billion, as shown in Exhibit III-2, plus currently unknown amounts for emerging, hard-to-value crimes like Internet fraud and computer crime. Exhibit III-3, which follows, expands upon each of the items listed in Exhibit III-2 and describes how each of the estimates were arrived at.

---

[4] *Mining Standards Task Force,* ***Setting New Standards: Interim Report****, Toronto Stock Exchange and Ontario Securities Commission, June 1998, pp. 75-76.*

Exhibit III-2

Summary—estimated value, relative size and growth rates for economic crime

Type of Crime	Estimated Value ($million)	Relative Scale/ Equivalence	Current Estimated Annual Growth Rate
Economic crimes where individual consumers and investors are the most common victims			
1. Securities fraud	$500 - 660	0.13% of the value of trading in stock exchanges.	Annual growth rate in the value of trading on Canadian exchanges, 1992 - 1997: 27%
2. Telemarketing fraud	$160 - 1,000	1.3% to 8% of the value of legitimate direct marketing sales	(Not available)
3. Internet fraud	(Not Available)	(Not available)	Forecast annual rate of growth in the number of Internet users making online purchases: 58%
Economic crimes where enabling business and public organizations are the most common victims			
1. Commercial fraud	$600+	0.2% of revenues of targeted companies	In line with overall business sector growth rates.
2. Computer crime	(Not Available)	(Not Available)	Annual rate of growth in computer security incidents noted by CERT (U.S.): 36%
3. Theft of tele-communications	$50 - 70	Approximately 0.5 - 1.0% of revenues.	Wireless telephone services growing at 19%, wireline at 8%
4. Offences against Federal statutes and programs[1]	~ $700 +	(not available)	(Not available)
5. Counterfeit currency	$7.8	0.003% of the value, and 0.013% of the volume, of notes in circulation	44% for face value of notes and 31% for volume of counterfeit notes.
6. Payment card fraud	$88	0.10% of net dollar volume on credit cards.	7% for value of fraud. 8% for volume of fraudulent cards.
TOTAL	**$2.1 - 3.1 bn.**		

(1. Tax evasion, Employment Insurance fraud, criminal bankruptcy and other government fraud. Estimate combines estimates of losses (bankruptcy and other government fraud), and losses prevented/recovered (tax and EI).))

These figure need to be viewed as "best guess" estimates, except in cases such as credit card fraud, theft of telecommunications and currency counterfeiting where the enabling organizations are able to quantify revenue gaps and/or physically monitor the outcomes from fraudulent activities. To the extent that information is available, we have cross-checked estimates from various sources to apply a basic "consistency and reasonableness test". Often however, estimates are made and published without any accompanying rationale; but this is to be expected to a certain extent given that criminal organizations do not have to disclose financial results or market share estimates.

Looked at from another perspective, that of the magnitude of potential losses prevented by successful policing, it is easy to see how the actual magnitude of economic crime may be much greater. For instance:

During April, 1994, the Canadian Combined Forces Special Enforcement Unit and Combined Forces Asian Investigation Unit arrested members of a Chinese syndicate that produced approximately 300,000 counterfeit (credit card) holograms, of which 250,000 had already been distributed. Based on the quantity delivered and using an estimated loss of $3,000 per card, Visa and Mastercard anticipated losses approaching $750 million caused by this group alone.[5]

Based on our allocation of crime types between individual consumers and enabling organizations, between $0.6 and $1.6 billion (29% to 52%) of the estimated total comes from individual consumers and investors, while enabling business and public organizations account for $1.5 - 1.6 billion. This suggests that in sectors where there are no major enabling organizations, the magnitude of fraud is significantly higher, and points to a need for a higher level of protection of these more vulnerable players. Where the enabling business and public organizations carry the biggest risks from fraudulent activity and have capabilities to monitor and prevent fraudulent activity, the magnitude of fraud is smaller.

This does not mean fraud against individual consumers is proportionately more prevalent (e.g., represents a higher proportion of revenues from the related economic sectors). Among the crime types that we have data for, losses are equivalent to 1% or less of legitimate revenues generated in the related economic sectors, with the exception of telemarketing fraud where the incidence may be as high as 8% of legitimate direct marketing revenues.

Another consideration is the fact that, with the increasing involvement of organized crime groups, economic crimes do not happen in isolation from each other, nor from other types of crime, such as drug dealing. For example:

"Three people have been arrested on 49 counts of manufacturing credit and debit cards and theft of telecommunication. The RCMP in Newmarket seized over 2,000 blank cards, equipment used to make credit and debit cards, and magnetic strip readers and writers. ... Mounties also seized pin hole cameras which had been placed in retail outlets above the cash register to record PINs as the customer entered it into the keypad. Various types of counterfeit identification, such as Ontario, Alberta and Florida drivers' licenses, social insurance cards and Ontario health cards were found as well as the equipment required to manufacture these cards. The two month investigation revealed thousands of cloned cellular telephones which allegedly were used by the accused for long distance calls to Iran, Lebanon and Kuwait. This resulted in millions of dollars in losses to the cellular telephone carriers. Cellular cloning equipment was also seized."[6]

---

[5]. *Keith Slotter, "Plastic Payments: Trends in Credit Card Fraud", **FBI Law Enforcement Bulletin**, June, 1997.*

[6]. *RCMP, Press release, April 28, 1998.*

Exhibit III-3-A
Commercial fraud

Estimated Magnitude

Approximately 57% of companies experience fraud and, in 1997, lost an average of $1.3 million per company. This suggests total fraud losses to Canada's biggest companies of at least $600 million per year.

- Between 52% and 62% of companies that participated in KPMG's four annual Fraud Surveys since 1995, reported being aware of fraud in, or against them. Sample size for these surveys, of between 210 and 300 companies, is relatively small so it is fair to say that the rate has remained relatively constant around 57%.
- Average losses to fraud reported by these companies in 1997 were $1.3 million, with one company defrauded out of $47 million. (If this company is excluded the average loss per company falls to $1.1 million.) KPMG analysts noted that the estimates provided were likely to understate the true level of commercial fraud.
- Assuming the companies participating in the survey are representative of all companies in the *Financial Post 1000* then fraud losses equate to approximately 0.2% of revenues, e.g., approximately $600 million. However, in 1996, the U.S. Association of Certified Fraud Examiners (ACFE) estimated that organizations lose about 6% of revenue to fraud and abuse (e.g. 30 times higher than the 0.2% level).
- Majority of financial losses to fraud occurred through a combination of:
  - Employee-related fraud—inflated expense accounts, secret commissions and personal use of company supplies.
  - Customer-related fraud—cheque forgery, credit card schemes, automatic teller fraud and kiting or lapping.
- Close to half of the participants in KPMG's fraud surveys between 1995 and 1998 have indicated that they expect fraud to increase in the next year. Most common reasons for this expectation in 1998: more sophisticated criminals, inadequate punishment, lack of emphasis on prevention, staff downsizing, economic pressures, weakening of society's values, and lack of government intervention.

Scale of Related Economic Sectors

- Sectors of the Canadian economy with the greatest concentration of commercial enterprises have enjoyed steady growth over the past five years. Rates of growth in real gross domestic product (e.g., with the inflation factor removed) in the main sectors for the period 1993 - 1997 were:

	Annual Growth Rates
Resources	+ 3.7%
Manufacturing	+ 4.6%
Construction Industries	+ 2.4%
Other Utility Industries	+ 1.7%
Transportation and Storage Industries	+ 2.8%
Communications Industries	+ 6.6%
Wholesale Trade Industries	+ 6.3%
Retail Trade Industries	+ 3.0%
Finance, Insurance and Real Estate Industries	+ 2.3%
Business Service Industries	+ 7.3%

*Sources: KPMG Investigation and Security Inc., **Annual Fraud Survey Reports**—1995 to 1998*
*Gips, Michael A., "Where has all the money gone?", **Security Management Online**, February, 1998. (www.securitymanagement.com)*

Exhibit III-3-B
Securities fraud

Estimated Magnitude	Scale of Related Economic Sectors
There are no reliable estimates of the value of securities fraud in Canada. U.S. data suggests annual losses could be $500 - 660 million. • No reliable estimates of securities fraud and market manipulation available for Canada. Majority of market manipulation efforts ("microcap fraud") are targeted at junior markets (Alberta (ASE) and Vancouver (VSE) exchanges, Canadian Dealer Network (CDN).) • In the U.S., a September 1997 Wall Street Journal article stated that *"Regulators now estimate annual losses (from penny stock fraud) to investors at more than $6 billion, triple the 1980s peak."* More recently, the North American Securities Administrators Association (NASAA) released a statement noting that *"State regulators now estimate securities fraud costs Americans nearly $10 billion a year, or about $1 million per hour."* • $10 billion in fraud is equivalent to 0.13% of the total value of trading on U.S. exchanges and NASDAQ. Applying the same percentage to the value of trading on Canadian exchanges gives an estimate of Canadian securities fraud of $500 million in 1996 and $660 million in 1997. The actual level of losses to fraudulent activity may be higher, given that listing and disclosure requirements in Canada's junior markets are not as extensive as that required for NASDAQ listings in the U.S. (However, it should be noted that Bre-X was also listed on NASDAQ.) Furthermore, Canada does not have uniform national regulation of its securities markets nor uniform listing requirements between its exchanges, which would provide for a consistent level of investor protection. • Bre-X is (hopefully) an extreme example of investor fraud, potentially involving losses well in excess of the annual estimate provided above. At its peak, Bre-X had a market capitalization of $6.1 billion. Gains by the perpetrators of the hoax represent only part of this value, and dollar losses by other investors, would have been substantially less also. • Performance of Canada's junior exchanges—ASE, VSE and CDN—was adversely affected by the fallout from Bre-X and falling gold prices during 1997. Value of trading fell by 35%, 25% and 13%, respectively, over 1996 levels. In contrast, value of trading on the Toronto exchange (TSE) grew by 40% in 1997 and 23% on the Montreal exchange (MSE.)	• Value of trading on Canadian stock exchanges (TSE, MSE, ASE, VSE and CDN) totaled $510.6 billion in 1997, on a volume of 43.9 billion shares. • Average annual rate of growth in trading value was 27% from 1992 to 1997. Average annual rate of growth in share volumes was 13.4% for the same period. • To put this in context, the value of trading on U.S. exchanges and NASDAQ was $US 7,807 billion in 1996 (compared to $384 billion for Canadian exchanges). Value of trading on NASDAQ grew at average annual rate of 38% between 1992 and 1993. 1997 growth on 1996 was 36%.

Sources: *TSE, MSE, ASE, VSE and CDN,* ***Annual reports*** *and* ***market summaries****.*
NASDAQ, ***1997 Annual Report, and 1997 Fact Book: Market Data****. (www.nasdaqnews.com)*
Schroeder, Michael, "Penny stock fraud is again on a resurgence", ***Wall Street Journal****, September 4, 1997.*
NASAA, "With Dow over 9,000, investors urged to be on guard for fraud", Press statement, 1998 (www.nasaa.org/investoredu/informed investor/dow9000f.html)
Mining Standards Task Force, Setting New Standards, Interim Report, Toronto Stock Exchange and Ontario Securities Commission, June 1998.

Exhibit III-3-C
Telemarketing fraud

Estimated Magnitude

Telemarketing fraud losses are at least $160 - 200 million, and may be as high as $1 bn.

- Police involved with telemarketing fraud believe that about 10% of victims report their experiences.
- Statistics on incidences of telemarketing fraud notified to Phonebusters statistics show:

Year	**Canadian Victims***		**U.S. Victims****	
	#	**Average Loss ($)**	**#**	**Average Loss ($)**
1995	4,038	$2,190	(N/A	(N/A)
1996	2,992	$3,461	922	$2,700
1997	2,182	$3,530	1,902	$2,154

(* "prize fraud"; **"prize fraud" plus "loan offers")

- Phonebusters figures suggest the number of Canadian victims of telemarketing fraud is decreasing, at an average annual rate of 26% between 1995 and 1997, but average losses per victim are increasing. Targeting of U.S. victims from Canada is increasing; according to the U.S. National Consumers League. Rankings of Canadian provinces as locations for fraudulent telemarketers in recent years:

Province	**1997 Rank**	**1996 Rank**	**1995 Rank**
Ontario	4	8	20
Quebec	6	3	25
British Columbia	8	9	10
Alberta	11	29	("obscurity")

Tightening of U.S. law relating to telemarketing fraud, combined with more intensive regulation and policing is believed to have pushed telemarketing fraudsters into Canada from the U.S.

- If, as police and industry stakeholders believe, the number of reported victims and losses represents 10% of the actual level then total losses for prize fraud among Canadians are of the order of $80 - 100 million per year. Telemarketing fraud cases uncovered by the FBI's "Senior Sentinel" program found that close to 50% involved prize fraud; with the balance being accounted for by bogus product offers, "charity rooms", "recovery rooms" and "rip and tear" schemes. This suggests total annual consumer losses in Canada of the order of $160 - 200m.
- Other estimates place the value at $300 - 1,000 million based on 10% of estimated U.S. losses. The Canada-United States Working Group on Telemarketing Fraud estimated that fraud accounts for as much as 10% of the total volume of telemarketing (e.g., 1 in 10 calls are fraudulent in nature).

Scale of Related Economic Sectors

- Telemarketing is a subset of the direct marketing industry.
- Data compiled by the Canadian Direct Marketing Association (CDMA) for their members (~750 corporate members responsible for over 80% of direct response marketing sales in Canada) show that the legitimate direct marketing industry has exhibited strong growth in recent years:
- Value of sales by CDMA members:

Year	**Sales**	**% Change**
1994	$9.7 bn.	
1995	$10.1 bn.	+4.1%
1996	$11.2 bn.	+10.9%
1997	$12.5 bn.	+11.6%

Average annual growth rate: +9%.

- Telemarketing's share of these amounts is not available.

Sources: *Canadian Direct Marketing Association, **1996/97 Annual Fact Book**, CDMA, Don Mills, Ontario, 1996. Plus supporting press releases.*
***Phonebusters: National Task Force Combating Telemarketing Fraud**, North Bay, Ontario. (www.gov.on.ca/phonebusters)*
***Report of the Canada-United States Working Group on Telemarketing Fraud**, Competition Bureau, Industry Canada, 1997.*
*Federal Bureau of Investigation (FBI), **Telemarketing Fraud: Senior Sentinel**, Washington DC, no date. (www.fbi.gov/majcases/telefrad/telfrad.htm)*
*Federal Trade Commission, **Fighting Consumer Fraud: The Challenge and the Campaign**, Washington DC, January 1997. (www.ftc.gov/reports/Fraud/index.htm)*
*National Consumers League, **1997 Telemarketing Scam Statistics**, Washington DC, 1998. (www.fraud.org/telemarketing/telestat.htm)*

Exhibit III-3-D
Internet fraud

Estimated Magnitude	Scale of Related Economic Sectors
There are no reliable estimates of the incidence rate or magnitude of Internet fraud. Numbers of complaints are growing rapidly in the U.S. • Internet provides a new way of committing traditional fraud activities; potentially more efficiently and on national or international basis, and significantly more complex for the law to investigate. • Little information available on the actual incidence rate or magnitude of fraud committed over the Internet. Fraud committed via the Internet can span the range from securities/investment fraud to commercial fraud to variations on telemarketing fraud. • The U.S. Internet Fraud Watch reported in January 1998 that the Watch had received 1,152 reports of possible Internet fraud in 1997, which was three times as high as 1996 complaints. • Most realistic proxy indicator for the future rate of growth in Internet fraud is probably the expected rate of change in numbers of Internet users making purchases online. IDC forecasts that the number of such purchasers would grow from 7 million in 1996 to 68.25 million by the end of 2001. This is equivalent to an average annual rate of growth of 58%. • *"... traditional financial crimes, such as multi-level marketing frauds, investment frauds, stock manipulations, credit card frauds, and copyright violations, as well as gambling, have simply found a new medium on the Internet. Investment frauds comprise a vast amount of the financial crimes identified on the Internet."* (Charles Owens, FBI, March 1997)	• Growth forecasts for e-commerce on the Internet vary tremendously. For example: – IDC forecasts that "web commerce" will go from an estimated $US 2.6 billion worldwide in 1997 to $US 220 billion in 2001—an annual growth rate of 203%. – Forrester research forecasts that business-to-business e-commerce will go from $US 8 billion in 1998 to $US 327 billion in 2002—an annual growth rate of 153%. – Morgan Stanley forecast (in 1997) that retail commerce on the Internet would go from $US 600 million in 1996 to $US 35 billion in 2000, for an average annual growth rate of 176%. This is the market segment that is most expected to attract the attention of Internet fraudsters. • Online banking, via the Internet, is expected to grow rapidly, in both the U.S. and Canada. For example, a 1997 survey by the General Accounting Office (GAO) found that about 7% of U.S. banks currently offer on-line banking services, but 47% plan to offer such services by the end of 1998. The risks associated with this trend are substantial: *"Online banking can expose bank and customer information and transactions to risks from electronic interception, data corruption, or fraud because of the widespread access characterizing these systems."*

Sources: *Blackburn, Wayne, "Fraud on the Internet", **CGA Magazine**, October 1997. (www.cga-canada.org/CGAMagazine/oct97/fraud_e.htm)*

*Grant, Susan, **Fraudulent Schemes on the Internet: Remarks to Senate Permanent Committee on Investigations**, National Fraud Information Center/Internet Fraud Watch Programs, Washington DC, 1998. (www.fraud.org/internet/intstat.htm)*

International Data Corporation (IDC), "Dramatic Growth of Web Commerce—From $2.6 billion in 1996 to more than $220 billion in 2001", Press release promoting forecasts from IDC's Internet Commerce Market Model, May 1998. (www.idc.com/f/HNR/ic2001f.htm)

*Forrester Research, **Sizing Intercompany Commerce Report**, Cambridge, MA, July 1997. (www.forrester.com)*

*Morgan Stanley & Co., **The Internet Retailing Report**, New York, May 28, 1997. (www.ms.com)*

*Owens, Charles L., **Computer Crimes and Computer Related or Facilitated Crimes**, Statement to the Subcommittee on Technology, Terrorism and Governmental Information, Committee on the Judiciary, FBI, Washington DC, March 1997. (www.fbi.gov/archives/congress/compcrm.htm)*

*General Accounting Office (GAO), **Identity Fraud**, Washington DC, May 1998, Report #: GGD-98-100BR and **Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking**, January 1998, Report #: GGD-98-34.*

Exhibit III-3-E
Computer crime—unauthorized access to computer/mischief to data

Estimated Magnitude	Scale of Related Economic Sectors
There are no reliable estimates of the incidence rate or magnitude of computer crime in Canada. Reported U.S. incidents suggest an annual growth rate of 36%. • No estimates of the incidence or magnitude of "hacking" crimes in Canada have been published. • A joint FBI/Computer Security Institute survey published in early 1998 found: – 64% of companies responding experienced an unauthorized use of their computer systems in the previous 12 months, up from 48% in their 1997 survey and 42% in their 1996 survey. – Almost 40% experienced 5 or more such incidents. – Internet systems are increasingly the target point of attack and for access to internal systems. – Attacks spanned the range from: unauthorized access by employees (44%), denial of service attacks (25%), system penetration from outside (24%), theft of proprietary information (18%), financial fraud (15%), and sabotage (14%). – Only 42% of those experiencing computer crime could quantify the losses. Average loss amongst those companies that provided estimates was just under $1 million. – Respondents believe the most likely groups to target them are: disgruntled employees (89%), independent hackers (72%), U.S. competitors (48%), foreign competitors (29%) and foreign governments (21%). – Only 17% of computer intrusions experienced were reported to law enforcement agencies. • Number of computer security incidents reported to CERT (Computer Emergency Response Team) Coordination Centre at Carnegie Mellon University has risen from 252 in 1990 to 2,134 in 1997, giving an average annual growth rate of 36%. • The capability of hackers to attack large numbers of systems with greater efficiency is increasing, via the use of IMAP attacks that enable intruders to launch large scale automated scans against networks. For example, the 1997 incidents recorded by CERT involved more than 146,000 sites. • FBI reports that it has over 500 pending computer crime cases, up from less than 125 one year ago, and computer crime arrests have increased 900% in the last two years as the number of dedicated investigators has grown.	• Organizations in every sector of the economy are vulnerable to computer crimes. • Very few organizations have security procedures in place to limit their risks, according to Ernst & Young's 1998 Global Information Security Survey. E&Y found that 53% of the participating IT executives did not monitor online activities, and 36% were not monitoring for network intrusions. 64% do not have planned incidence response strategies in place.

Sources: *Computer Security Institute, "1998 CSI/FBI Computer Crime and Security Survey",* ***Computer Security Issues & Trends,*** *Vol. IV, No. 1, 1998. (www.gocsi.com).*
CERT® Coordination Center, ***1997 Annual Report (Summary),*** *Carnegie Mellon University, 1998. (www.cert.org/annual_rpts /cert_rpt_97.html) Statistics on incidents reported to CERT are available at www.cert.org/stats/cert_stats.html).*
Ernst & Young International, ***1st Global Information Security Survey****, 1998.*

Exhibit III-3-F
Theft of telecommunications

Estimated Magnitude	Scale of Related Economic Sectors
Estimated annual losses to telecommunications theft are about $50 - 70 million. • Estimated incidence rates are less than 1% of revenues for wireline services and between 1% and 2% for wireless services. • This results in estimated annual losses of approximately $50 to $70 million. • Canadian incidence rates for wireless theft are lower than U.S. rates, which are reported by the Cellular Telecommunications Industry Association (CTIA) to be equivalent to 3.8% of revenues. U.K. and European telecommunications operators estimate their losses to be about 2-3% of revenues. • In the U.S., the CTIA and law enforcement agencies have been successful in reducing the incidence of cloning fraud in recent years. However, subscription fraud, which is much simpler to commit, is continuing to grow. Canada is also experiencing an increased rate of subscription fraud .	• Total revenues in the telecommunications sector grew at an average annual rate of 7% between 1990 and 1996, with growth rates accelerating in the second half of this time period. 1995 long distance and international revenues were $8.3 billion and wireless revenues were $2.1 billion. • Long distance wireline service revenues grew at an average annual rate of 8% and wireless revenues grew at 19%. • Growth rates in wireless are expected to stay at this level, or increase, in coming years, with the introduction of digital wireless products and an increased number of competitors in the market. • Convergence of telecommunications and computing technologies also means that cable and satellite television services face many of the same risks as telecommunications carriers. Annual cable revenues were $2.7 billion in 1996, and grew at an average annual rate of 9% over the period 1990 to 1996.

Sources: *Spectrum, Information Technologies and Telecommunications Sector, Industry Canada,* ***Information and Communications Technologies: Statistical Review, 1990 - 1996****, Ottawa, February 1998. (strategis.ic.gc.ca/infotech)*

Milstone, Erik, "Subscription Fraud Looms", ***Wireless Week****, October 6, 1997.*

CTIA, Wireless ***Telephone Fraud Frequently Asked Questions****, www.wow-com.com/professional/fraud/Ffaqs.cfm*

Purton, Peter, "Fraud and Theft", ***Financial Times****, June 10, 1998. (Part of a Financial Times survey on the telecommunications sector.)*

Exhibit III-3-G
Federal statutes and programs

Estimated Magnitude	Scale of Related Economic Sectors
Amounts recovered (losses prevented) for income tax evasion and EI fraud represent approximately $527 m. Criminal bankruptcies are estimated to involve another $62 m., and other government fraud approximately $100 m. **Tax evasion** • Revenue Canada's Special Enforcement Unit recovers approximately $50 million per year in evaded taxes, much of which is linked to illegal business activities. This unit's first priority is the recovery of taxes owing to the Crown, not necessarily criminal prosecution and punishment (other than tax penalties). Moneys are recovered through a combination of administrative powers (via the Income Tax Act) and criminal investigations and prosecutions. • Revenue Canada does not publish estimates of unpaid taxes linked to illegal economic activities. (Note: Investigation of criminal tax evasion was recently transferred from being within the mandate of the Economic Crime Program to the Integrated Proceeds of Crime (IPOC) Program.)	• Income taxes collected by Revenue Canada totaled $148 billion. Individual income tax payments (including Employment Insurance premiums) represented 86% and corporate payments 13%.
Employment Insurance fraud • HRDC's Employment Insurance (EI) investigation and enforcement unit conducts reviews/investigations of close to 1 million EI files per year. When cases of knowingly committed abuse are identified the unit has four options: issue a warning letter, impose an administrative penalty, obtain a summary conviction under the EI Act, or refer to the RCMP for a Criminal Code investigations. • Estimated pay-off from investigations was about $575 million in 1997-98, composed of: (1) Recovery of overpayments ($228.5 m.) and receipt of penalty payments under the EI Act (about $85 m.). (2) Avoidance of future payments that would have otherwise gone to perpetrators of EI fraud, which was estimated to have a present value of $248.9 m. This information shows that estimated losses prevented amounted to $477 million in 1996-97. • Approximately 250 EI Act prosecutions per year resulting in fines of about $1 million. About 20 other cases, per year, referred to the RCMP. Cases are referred to RCMP to obtain convictions (not necessarily to recover fraudulent payments) as part of a visible deterrence-creation strategy. • HRDC does not publish estimates of total EI fraud.	• Employment insurance premiums received by the federal government: 1993-94 $18.7 bn. 1994-95 $19.4 bn. 1995-96 $18.9 bn. 1996-97 $20.3 bn. • Total benefit payments in recent years were: 1993-94 $17.6 bn. 1994-95 $14.8 bn. 1995-96 $13.5 bn. 1996-97 $12.4 bn.

Exhibit III-3-G (cont'd)
Federal statutes and programs

Criminal bankruptcy • Office of the Superintendent of Bankruptcy refers approximately 230 bankruptcies to RCMP for investigation each year, under the Bankruptcy Act or Criminal Code, the majority of which are business bankruptcies. Number of investigations is equivalent to about 1.8% of all business bankruptcies. • Completed RCMP bankruptcy files show an average estimated value of $271,000 per case, giving a total value of the amounts involved in bankruptcy investigations of about $62 million.	• Total number of bankruptcies fell in the mid-90s and is now rising again, primarily due to trends in the number of consumer bankruptcies. Total number of bankruptcies in 1997 was 97,497 of which 12,200 (13%) were business and 85,297 (87%) were consumer. Rate of business bankruptcy varies within the range of 12 - 16 bankruptcies per thousand businesses.
Other government fraud • Other government fraud covers such areas as fraud related to loans and funding provided to a wide array of business and economic organizations, and breach of trust and corruption investigations. There are no published estimates as to the value of this mix of fraudulent activities. The RCMP estimates that this mix of fraud, breach of trust and corruption cases has a value of approximately $100 million.	

Sources: 1997-98 Performance Reports for Revenue Canada, Human Resources Development Canada, and Industry Canada.
RCMP case files.

Exhibit III-3-H
Counterfeit currency

Estimated Magnitude	Scale of Related Economic Sectors
Face value of counterfeit Canadian notes seized or detected was $6.1 million in 1997, plus another $US 1.2 million in U.S. notes. • Total volume of counterfeit Canadian notes seized by police or detected in circulation has been growing at an average annual rate of 31% since 1992. 109,881 notes were seized or detected in 1997. • During the 1992 -1997 period, the total face value of counterfeit Canadian notes has varied between $996 thousand (1992) and $2.96 million (1994), and an exceptionally high value of $6.1 million in 1997. Underlying rate of growth has averaged 44% per year since 1992. • Value of U.S. notes seized or detected in circulation in Canada has varied from a low of $US 324,345 (1996) and a high of $US 118,469,883 in 1995. 1995 outcome was exceptional, and due to two significant seizures in Montreal. 1997 amount had a face value of $US 1.2 million (~ $CDN 1.7m.) • Technical capabilities of counterfeiters to copy security features on Canadian and U.S. bank notes are continually increasing, e.g., ability to replicate OSD (optical security device) features. Availability and accessibility of this technology is becoming easier and cheaper.	• Canada had a total of 815 million currency notes in circulation in 1997. Counterfeit notes seized or detected represent 0.013% of the total volume. The volume of notes had been increasing at an average annual rate of 1.4% since 1992. • The average net value of currency (using the Bank of Canada's M1 measure) has been growing at a rate of 5.7% over the same period. The value of notes seized has varied between 0.003% and 0.022% of the net value of currency over this period.
Sources: Table B4—Statistics Pertaining to Counterfeit Bank of Canada Notes, ***Bank of Canada Review****, Spring 1998.* *RCMP web site—Counterfeiting (www.rcmp-grc.gc.ca/ntml/counter.htm)*	

Exhibit III-3-I

Estimates of the magnitude and scale of economic crime—payment card fraud

Estimated Magnitude	Scale of Related Economic Sectors
Cost to financial institutions for credit card fraud was $88 million in 1997 • Write-offs by issuing institutions for fraudulent use of credit cards was $88.1 million in 1997. • Write-offs have been growing at an average annual rate of 7% since 1992. However, the rate of growth in legitimate credit card transactions was 12.4% per year over the same period. This means that fraud losses have fallen from a level equivalent to 0.14% of net dollar volume on credit cards (retail sales transactions plus cash advances) in 1992 and 1993 to 0.10% in 1997. • Number of fraudulently used cards in 1997 was 90,000. The number of fraudulent cards grew at an average annual rate of 8% from 1992 to 1997. This growth has outpaced the rate of growth in the number of cards in circulation so that the 1997 volume of fraudulent cards has increased from a level equivalent to 0.25% of issued cards in 1992 to 0.28% in 1997. • Counterfeit cards are increasing in significance (vs. stolen cards and fraudulent applications)—up from 10% of fraudulently used cards in 1992 to just over 40% in 1997. • Canadian losses to fraud are in line with those of other developed economies, e.g., 1997 losses in the UK represented 0.09% of transactions, losses by Visa members in the U.S. represented 0.097% of billing transactions in 1997, and worldwide Mastercard losses represented 0.11% of total billing transactions in 1997. Counterfeiting is the fastest growing type of card fraud in both the U.K. and U.S. • Debit card fraud is an emerging risk, as dependence on these cards increases and the value of transactions grows.	• Net dollar volume on credit cards (retail sales transactions plus cash advances) was $84.3 billion in 1997, up from $46.9 billion, giving an average annual growth rate of 12.4%. • Number of cards in circulation has been growing at an average rate of 5.5% per year between 1992 and 1997, from 24.4 million in 1992 to 31.9 million cards in 1997. • Interac Association reports that the annual dollar values of Interac direct payments has been growing at a rate of almost 40% per year since 1995. Reported incidents of debit card fraud are not high but are believed to be growing quite rapidly. An article in the September 1997 edition ***of Credit Card Management*** reported that *"Though US debit card fraud losses remain low – about $70 million last year compared with about $745 million for credit cards – there is mounting pressure on financial institutions to do more to protect their cardholders."*

*Sources: Canadian Bankers Association, **Credit Card and Credit Card Fraud Statistics**, 1998. (www.cba.ca)*

*"Plastic Card Fraud on the Increase Again", **Financial Times**, April 4, 1998, London Edition.*

*Slotter, Keith, "Plastic Payments: Trends in Credit Card Fraud, **FBI Law Enforcement Bulletin**, June 1997, (www.fbi.gov/leb/june971.htm)*

*General Accounting Office (GAO), **Identity Fraud**, Washington DC, May 1998, Report #: GGD-98-100BR.*

*Green, Jeffrey, "The Fraud War Goes High Tech", **Credit Card Management**, Volume 10, No. 6, September 1997, pp24-28.*

3. Economic and social impacts are widespread, harmful and reach into the very structure of the economy

As we noted in Exhibit III-1, the impacts of economic crime can be categorized under three headings—impacts on individual consumers and the public; impacts on enabling business and public organizations; and, impacts on the economy in total. In our interviews and literature review it was apparent that most impacts are common to all types of economic crime. Unfortunately, no one that we are aware of has attempted to quantify these impacts, yet.

a) Impacts on individual consumers and the public

- Loss of savings and assets.
- Increased reliance on the public safety net, e.g., due to losses of retirement savings to fraudsters.
- Disruption to personal life and income generating activities.
- Needs to re-establish "financial identity" in the wake of fraudulent use of victims' credit cards, telephone numbers, and resulting denials of service, etc.
- Higher costs for products and services.

b) Impacts on enabling business and public organizations

- Loss of revenues and income.
- Higher operating and financing costs, which may or may not be passed onto customers in the form of higher prices and fees.
- Higher costs of R&D, in order to improve integrity of products and systems, and introduce product improvements on a more frequent basis than would otherwise be the case.
- Disruption or damage to computer systems that rely upon computer and telecommunications networks. In turn, this damage or disruption may result in:
  - Loss of business and customers.
  - Endangerment of human lives.
  - Breaches of national security.
  - Loss of goodwill and erosion of companies' market valuations.
- Losses of intellectual property (as a result of computer security breaches).

c) Impacts on the economy in total

- Reduced levels of direct (income) and indirect (GST) tax revenues, leading to higher debt servicing costs, or a longer time period for deficit elimination.
- Redirection of income from high savers to low savers, and from sound investments to risky or illegal investments, leading to adverse economic growth.
- Growth of less-regulated, parallel financial markets and channels that facilitate money laundering and international transfers.
- Erosion of public confidence in the integrity of Canada's economic infrastructure, e.g., loss of confidence in the security and transparency of stock markets, the use of plastic and electronic payment systems, the security of wireless telephone networks, the honesty of business and government officials, etc.
- Loss of attractiveness, and competitiveness, as a country to invest in or do business in. Carried to an extreme this would result in a loss of the high ranking Canada enjoys in the World Economic Forum's annual Competitiveness Index (#5 in 1998 behind Singapore, Hong Kong the United States and the United Kingdom, and #4 in 1997) or the annual Transparency International Corruption Perception Index, which gave Canada a score of 9.1 out of 10 in 1997, behind only Denmark, Finland, Sweden and New Zealand.[7]

Another way of looking at the impacts of economic crime is to consider what might have happened if the estimated value of losses to economic crime presented in Exhibit III-2, of $2.1 to $3.1 billion, had been available for spending, investment or disbursement in legitimate consumption and investment activities. Probable impacts, and consequences, include the following:

For individual consumers and investors who would have otherwise been victims of fraud:

- Consumer spending and investment by individual consumers and investors in the legitimate economy would probably be least $700 - $1,700 million higher. In turn, this spending and investment would have made generated substantial business growth and job creation in the retail, wholesale, manufacturing and securities industries.

---

[7] *World Economic Forum, **Global Competitiveness Report 1998**, Geneva, Switzerland, 1998.*
*Transparency International, **1997 Corruption Perception Index**, Berlin, 1997.*

- These consumer expenditures would generate additional GST revenues for the federal government and provincial sales tax revenues for provincial governments. In turn, the associated business and employment growth would produce additional income tax revenues and stimulate further consumer and business expenditures.

For enabling business and public service organizations that would otherwise have been victims:

- Lower operating costs for enabling business and public service organizations, due to reduced losses to economic crime and, potentially, a lower rate of spending on measures to prevent economic crime incidents.

- Lower fees and interest charges for consumers, reflecting the fact that they would no longer have to collectively carry the costs associated with preventing, detecting and deterring economic crime targeted at enabling organizations.

- Reductions in the costs of enabling organizations' transactions monitoring and investigation activities, and costs of research and development to improve the security and safety of business systems, services and products or a less frequent rate of introducing security upgrades to products and services.

For Canada in general and the federal government:

- Lower disbursement levels on government programs – such as Employment Insurance, which also provides opportunities to reduce the cost of EI premiums – plus a more rapid rate of reduction in the federal deficit.

- A better perception of Canada as a place to invest among international investors, leading to higher rates of investment and trading activities on Canadian stock exchanges. Domestically, an improved image for the stock market as a secure place to invest savings and accumulate retirement assets.

- Improved perceptions regarding the use of new forms of commerce, such as e-commerce, leading to a more rapid rate of growth in adoption and use of these services.

- Reductions in the amount of money going into the financing of other illegal activities with the potential for further distortion of the economy, leading to less misleading monetary data and performance signals for use by economic policy makers.

Once again, illustrations from specific cases and research point to the way economic crime impacts on victims and on the integrity of the national economic infrastructure.

On the impacts of computer crime:

"Really great answers do not exist; losses in these types of scenarios are difficult to estimate. At a minimum, there will be manpower costs (sometimes very large in magnitude) involved in investigating the incident to determine exactly what happened, whether the intruders still have access (and if so, to what), etc. In addition, machines may have to be shut down, services moved from one host to another, and so forth while the incident and investigation are taking place—this can result in significant loss from inability of employees to use computing/network resources.

Also, the corporation may suffer loss of reputation and customer confidence as a result of the incident, something that can be the most costly of all outcomes. Consider, for example, the effect of an intrusion into a bank on current and potential customers' willingness to do business with that bank. Finally, the cost of bringing in lawyers and cooperating with law enforcement can also be significant. The total loss resulting from a few intrusions into a corporate network can, therefore, be extremely costly—perhaps in the range of millions of dollars."[8]

On the impacts of telemarketing fraud:

Telemarketing fraud, which generally has a transborder nature and scope, has become an operational priority of all of the policing agencies in the Montreal metropolitan region. The RCMP, Sûreté du Québec and SPCUM have established a combined investigative team to maximize efforts to combat this challenge. The team works closely with representatives from all levels of government, as well as with counterparts in the FBI and US Customs. Since 1995, efforts in this program area have led to the return of $7.5 million dollars to American and Canadian victims of this crime. Future efforts will build upon this success through traditional investigations, as well as through increased cooperation with US agencies to accelerate cross-border extradition.

---

[8] *Schultz, Dr. E., Quoted in: "1998 CSI/FBI Computer Crime and Security Survey",* ***Computer Security Issues & Trends****, Vol. IV, No. 1, Winter 1998, p. 11.*

On the impacts of cable television services (theft of telecommunications) using altered decoders:

The Vancouver Commercial Crime Section recently completed a successful investigation into the manufacture and sale of "altered decoders" for cable television services that, once installed, enabled users to receive pay television and pay-per-view television services at no cost.

Between 1993 and 1997 the twelve principals in this activity purchased, modified and re-sold approximately 30,000 converter units. The purchase cost of these units to the gang was approximately $3,000, 000 . Following modification the units were sold to final users for approximately $225 - $300 per unit, giving gross sales of $6.75 - 9.0 million and a gross margin of between $3.75 and $6.0 million. Distribution and sale of the converters was facilitated by a network of approximately 40 associates of the gang members.

Additionally, owners of the altered decoders were able to avoid paying providers of cable television services in the Vancouver area. Estimates prepared by one of the service providers suggests the revenue foregone, if all 30,000 units were being actively used, would have been of the order of $54 million, of which about 70% would have gone to the program suppliers and 30% to the cable service. This is based on an estimate of the amount of television service consumed per month and the retail charges for these services, to arrive at a total monthly gross revenue loss of about $160 per decoder (approximately $50-60 per month for pay television services and about $100 per month for pay-per-view services).

Foregone tax revenues would have amounted to approximately: $3.78 million in GST, $3.78 million in PST, $0.5 million in municipal levy, and $0.15 million in cable fees paid to the CRTC)

4. Stakeholders see a variety of emerging challenges and expanding threats; many are linked to opportunities created by new technologies

A number of common challenges and expanding threats were encountered in our research and interviews. These challenges and threats are expected to drive much of the more complex, and potentially costly, aspects of economic crime in coming years. Law enforcement agencies, regulatory agencies, enabling business and public organizations will need to be prepared, or better prepared, to meet them. Greater understanding of the issues among the public, and in political and legal systems, will need to be developed. Ongoing public education and communication on the implications of economic crime should provide the first step in minimizing the incidence of these criminal activities.

The key emerging challenges and expanding threats are:

a) Increasing involvement of organized crime groups

Organized crime groups are increasing their involvement in economic crime activities, exploiting opportunities across all categories of economic crime. These organized crime groups go beyond the traditional stereotypes to include a wide variety of groups, often, but not always, organized by ethnic group. Many of these groups support their operations with extensive use of computer systems, e-mail and other sophisticated communications technologies, in the same way that legitimate businesses do. Unlike many legitimate business organizations economic crime groups are very flexible, highly responsive to change and willing to switch from one type of criminal activity to another as the intensity of policing changes.

b) Globalization of economic crime

Economic crime is increasingly a global business, working off the globalization of legitimate business and global nature of electronic networks. New communications technologies enable even small business operators and fraudsters to extend their reach to adjoining provinces, to adjoining countries or around the world. In turn, this moves many otherwise small and locally-oriented crimes into the national or international arena and under the authority of national police forces. Unfortunately, resources are not transferred as well to respond to this structural change in the nature of policing demand.

c) Increasing threat of computer crime to business networks and infrastructure

Threats to the functioning of the electronic infrastructure for business from computer crime are increasing, as business dependency on wide area networks and supporting technologies increases. As business systems increase their reliance on electronic systems the risk of damage or disruption from unauthorized access or mischief to data attacks increases. As noted above, the potential consequences of such events can be financially disastrous for many businesses.

d) Low levels of concern among many business and government organizations

Many fraud and security surveys have found a significant number of organizations that either are unaware of the risks they face or do not have the systems in place to minimize risks of fraud, from both internal and external sources, of breaches of computer security. This issue should be of particular concern to the senior executives of business organizations and their boards of directors, given that a high proportion of fraud against businesses (and presumably government departments and agencies) is committed by employees. For example, KPMG's 1998 Fraud Survey found that 77% of respondents identified employees as a source of fraud, much higher than customers (39%), service providers (14%) and suppliers (14%).

e) New security technologies can facilitate the work of crime groups at the same time as they help to protect against criminal intrusions

New technologies, such as encryption and security features on computer hardware and software can be a powerful aid to organizations needing secure communications. However, these same technologies can be used equally effectively to protect the communications and information of crime groups from external monitoring and intervention, which raises a number of key challenges to such key police methods as phone tapping. Similar concerns also arise over the potential for the next generation of payment cards – "smart cards" – as a more convenient and potentially untraceable vehicle for money laundering.

Stakeholders also face the challenge that many of the publicly-funded agencies—from regulatory agencies to police forces to the criminal justice system—are operating under severe resource constraints. Progress by one level will not necessarily result in an immediate improvement in the incidence rate of various crimes or an increased rate of prosecution and conviction. An end-to-end solution is necessary, not a piecemeal approach.

C. Current versus ideal positioning of the Economic Crime Program

The emerging environment for combating economic crime requires a different approach to the management of the Force's relationships with other stakeholders, bringing with it needs for new or altered priorities. In part, such changes are a function of the very issue posed at the beginning of this chapter, namely, what would happen if the RCMP did not have the resources required to fulfill its mandate?

This section addresses this question, by:

- Defining the typical roles of the different stakeholders, in terms of specific areas of focus, and unique capabilities, and the boundaries and possible overlaps between each type of stakeholder.
- Assessing the extent to which the Program is able to fulfill its mandate given current resource levels.
- Summarizing the most commonly expressed expectations among stakeholders as to the role the Force should be playing if it had optimal resources.

This is, by necessity, a qualitative analysis given the weaknesses in quantitative information, from both external sources and the Program's own performance data, on the incidence rates of different types of crimes and the relationship between the intensity of law enforcement and crime rates.

1. Typical stakeholder roles can be clearly differentiated

Exhibit III-4 summarizes the key roles each of the stakeholder groups typically concerned with economic crimes could, or should, be playing. It does not attempt to define all of the roles each type of organization attempts to play, only those where the particular stakeholder type can make a significant contribution. These contributions ultimately relate to either the prevention, monitoring, detection, investigation or prosecution of economic crimes.

A review of this information shows the following key roles, most of which are self-evident:

- ***Enabling organizations*** have the capability to monitor transactions and to identify and screen "red flag" suspicious patterns and incidents. Such cases may be investigated and completed by the organization or referred to a regulatory agency or police service for further investigation and/or prosecution. These organizations also have the capability to terminate customer service arrangements to prevent fraudulent activities continuing and, in the case of public agencies operating under the power of specific legislation and regulations, can impose administrative penalties and fines, for example, with the Employment Insurance program. As the point of contact with customers they also have the capability to inform and educate customers about the risks and best responses to fraudulent activities.

Exhibit III-4
Spectrum of stakeholder roles

Individual Consumers or Investors
(Potential Victims)

- Exercise due caution in economic activities.
- Report potential and attempted crimes.

Enabling Business & Public Organizations
(Service Providers)

- Educate customers on risks and responses.
- Monitor transaction patterns.
- Screen suspicious incidents; identify cases that warrant further investigation.
- Intervene to terminate low-level crime fraud attempts/activities.
- Investigate and refer qualified cases to regulatory agencies and/or police.

Regulatory Agencies & Bodies

- Monitor transaction patterns (may be in addition to, or in lieu of, monitoring by enabling organizaations).
- Investigate suspicious incidents and cases.
- Apply administrative penalties and enforcement actions.
- Refer potential criminal cases to police.

Police Services

- Collect and share intelligence.
- Monitor transaction patterns (may be in addition to, or in lieu of, monitoring by enabling organizations & regulatory agencies.)
- Investigate suspicious incidents and cases at local, provincial, national and international levels.
- Select cases to take forward for prosecution.
- Support prosecution.

Crown Counsel

- Assess merits of proposed prosecutions.
- Prosecute and convict.

Justice Departments

- Enact appropriate legislation and regulations.
- Negotiate and support multilateral agreements, harmonization arrangements and joint actions.

- However, not all types of economic crime involve large enabling organizations. In these cases, ***regulatory agencies*** may play a similar monitoring and screening role to enabling organizations in addition to undertaking compliance and screening investigations to maintain market efficiency, fairness and transparency. This includes powers to penalize errant behavior by market participants. Cases found to have grounds for criminal investigation are referred to police services for action.

- ***Police services*** have (or are expected to have) a capability to collect and share intelligence on criminal activities, and investigate cases leading to criminal prosecutions. Interactions between police services are also necessary, such that, cases are referred to the forces that either have jurisdiction for an investigation or that have the necessary skills and resources. Typically, the RCMP is looked to as the force to handle cases that are require national or international investigations or are technically complex.

- ***Crown counsel*** focus on the assessment of cases for prosecution and take the selected cases through the court system, resulting in goal sentences and/or the imposition of fines and restrictions.

- ***Justice departments*** provide the policy and legal framework for the functioning of regulatory agencies and police services. At the federal level, they also negotiate the arrangements under which Canadian police services can interact with the police services of other countries.

No single stakeholder organization has the lead responsibility for ensuring effective communication and coordination between the different groups. This reflects the fact that each set of stakeholders has a different set of objectives and priorities. Only the police and crown counsel services are primarily concerned with the prevention, investigation and/or prosecution of criminal activity while other organizations are primarily concerned with achieving commercial objectives or ensuring market mechanisms are functioning efficiently and effectively. Poor communications and coordination amongst stakeholders increases the risks of duplication of effort during investigations or the creation of parallel monitoring systems.

At the same time, a complete end-to-end solution is needed if the overall incidence of economic crime is to be minimized. Bottlenecks at one or more point in the progress of cases through different stakeholder levels can, and do, have the effect of weakening the overall efforts by all stakeholders to minimize the incidence and impacts of economic crime. Resource limitations and time delays affecting the regulatory agencies, police services and crown counsel services are seen to be major bottlenecks at present.

2. Stakeholders believe current RCMP resources are preventing the Program from achieving its mandate, and have had to take their own remedial actions

The short answer from most stakeholders to the question of what would happen if the RCMP did not have the resources required to fulfill its mandate was that the Force does not. That is, it is already in a position where resources are insufficient to optimally fulfill the Program mandate.

This resource shortfall has resulted in:

a) Expansion of monitoring and investigation activities by enabling business and public service organizations

Enabling organizations have had to expand their monitoring and investigation activities in order to detect apparent incidents and conduct investigations of such incidents up to the point where decisions on the merits of seeking criminal prosecution can be made. Early detection and intervention also facilitates the minimization of lost revenues.

Deployment of monitoring systems is a function that is well suited to the enabling organizations, because they have automated transaction processing systems (e.g., for processing credit card transactions or for telephone switching and billing) and can readily add sophisticated software to analyze transaction patters and identify "red flags". Many aspects of investigations, however, could be undertaken by either the Program of by the enabling organizations. Accordingly, they have felt compelled to expand their capabilities in this area.

However, it is not possible for the enabling organizations and regulatory agencies to take over the full range of activities that the Program is capable of. Skills in investigation and intelligence gathering, plus legal powers enjoyed by the Mounties as Peace Officers, provide them with some specific capabilities that are not substitutable. This capability has value to stakeholders. For example, the Program's joint pilot project with the B.C. Securities Commission and Regional Crown Counsel to more effectively combat illegal activities in the B.C. securities market has been held up as a prototype of the approach required for future partnership-based approaches to combating economic crime.

Transaction monitoring systems and methods are becoming highly sophisticated extensions of the basic systems used by enabling organizations to deliver and bill their services. Many stakeholders have increased their investment in this activity to increase the sophistication and data handling capacity of their surveillance systems, and, from the RCMP's perspective, it makes sense to encourage stakeholders to develop such systems where they are willing to do so and can afford to do so, rather than have the RCMP fund such development.

However, one stakeholder commented that, in relation to stock market trading, it was not necessary for the RCMP to develop its own monitoring tools to detect market manipulation when the exchanges themselves had the resources and need to develop and deploy sophisticated surveillance tools to monitor trading activity. Given this, they believed that client and public needs would be better served if the Program focused its efforts on investigating and prosecuting potential cases of market manipulation that were identified by the exchanges' surveillance systems.

An example of trends in this area is the following:

NASDAQ

"Trading activity is monitored by the StockWatch Automated Tracking System (SWAT^{SM}), a state-of-the-art automated trading surveillance system that tracks every trade second-by-second and can identify the specific computer terminal from which a trade was made. ...

(The) Fraud (team) also uses RADAR (Research and Data Analysis Repository system) and SWAT to conduct investigations of long-term price swings in Nasdaq and over-the-counter equity securities for fraud or manipulation. ...

NASD Regulation will become the first regulatory organization to systematically monitor the Internet for securities fraud when it implements NetWatch, its new automated Internet Surveillance System, in 1998. ... Using an intelligent information extraction tool with advanced natural-language-processing search capabilities, NetWatch will consistently and thoroughly scan the Internet and relate its findings to actual market activity and newswire stories."[9]

Monitoring of transactions where there are no large enabling organizations or regulatory agencies with the necessary resources and expertise, such as telemarketing fraud, is a different issue. As yet, there is no apparent solution to the challenge of how to best intervene on behalf of individual consumers to identify "red flags" other than through sustained consumer education leading to higher rates of incident reporting.

b) Loss of deterrence effects

Visible, sustained involvement by the RCMP in the investigation of apparent cases of economic crime has a powerful deterrent effect, quite independent of the actual outcomes from such investigations, according to many other stakeholders. As the volume of economic activity and economic crime has grown the level of involvement by the Program is perceived, by crime groups, to have fallen. This has had the effect of encouraging crime groups to expand their activities and increases losses to the enabling business organizations and individual consumers and investors.

---

[9] *National Association of Securities Dealers Inc. (NASD), **1997 Annual Report**, Pages 27, 33 and 34.*

c) Limited capability to respond to the increasing number of national and international crime activities

The following comment sums up another impact of the decline in the ability of the Program's resources to respond to evolving demands. It can be considered typical of the situation in many sectors affected by economic crime.

> *"Further, many (stock market) manipulations are instigated by individuals through offshore holding companies which means that detection and investigation must be handled by a police agency with a clear national and international mandate. The RCMP needs to commit the resources necessary to adequately investigate and prosecute these types of crimes in order to provide a strong deterrent effect. Particularly where difficult offshore jurisdictional issues arise, the RCMP needs to fulfill their mandate by carrying out investigations involving international components. Currently, there is little evidence to suggest that these types of investigations are being actively pursued by the RCMP."*

d) Extended time periods for investigations and low probabilities of conviction

As Program resources have become stretched to the limit, the time required to successfully undertake investigations and pursue prosecutions has become unsatisfactorily long, affecting the efficiency of investigations and likelihood of achieving convictions. This situation is further aggravated by resource limitations in the Crown Counsel services, thus compounding the bottlenecks and conviction rates. The result is frustrated Program investigators, frustrated stakeholders and reduced risks to perpetrators.

e) Increasing reliance on administrative penalties and civil remedies, with declining success in controlling activities of organized crime groups

Where possible, enabling organizations and regulatory agencies have relied upon the application of administrative penalties and civil remedies as a way of limiting the incidence of economic crimes. However, repeat offenders and organized crime groups have continued, and expanded, their operations, because the potential for significant financial returns outweighs the risk of criminal prosecution.

f) Rising popularity of Canada as a base for certain types of international economic crime

Canadian laws, and requirements for prosecution and conviction, relating to economic crime have not been updated to the same extent as those of other developed countries, particularly those of the U.S. Consequently, as criminal operations have become more difficult to undertake they have been exported to more accommodating international locations. For example, since the U.S., tightened its federal law relating to telemarketing fraud, Canada has gone from having one province in the "top 10" locations for telemarketing fraudsters in 1995 (B.C. was rated 10th) to having four provinces in the "top 11" in 1997 (Ontario – #4, Quebec – #6, B.C. – #8 and Alberta – #11).[10]

g) Unmet needs for proactive intelligence gathering and dissemination

Most stakeholders stated that this function was not being performed at all, or on a sporadic basis at best. Most then went on to say that better intelligence would enhance the ability of both the RCMP and stakeholders to keep economic criminals on a defensive footing. Good intelligence should enable the Force to play a more proactive role, in partnership with other stakeholders.

The benefits of good intelligence are aptly summarized in the following statement by the Director General of the U.K.'s National Criminal Intelligence Service (NCIS):

> *"(There is a) need to change our methods of policing to fit the new technological age.* ***Instead of following up reported crimes, it will benefit us far more to be ahead of the game and intelligence-driven****. We need specialist officers with technical knowledge and expert support. This coupled with mutual support between law enforcement and industry will, we believe, meet the new policing challenge of the next millennium."*[11] *(Emphasis added.)*

At the same time, many stakeholders stated that they had the highest respect for the abilities and dedication of individual officers and their efforts in the face of resource constraints and management processes. The issue is not one of the performance of the individual officers but one of the achieving optimal efficiency for the Program in its entirety.

3. Stakeholders are looking to RCMP to play a leadership role

In terms of relative priority, most stakeholders were of the view that the RCMP should be focusing on:

- Cases involving organized crime groups that account for significant losses or disruption. In other words, "go after the big guys, and send a strong deterrence message to the little guys." The mere involvement of the Force in economic crime investigations carries a deterrence effect.
- Cases that have national and international components, and are typically more complex and require higher levels of technical expertise, which is often not present in provincial or municipal police forces.

---

[10] *National Fraud Information Centre, 1997 Telemarketing Scam Statistics, Washington DC, 1998. Ratings are based on the numbers of complaints received by the Centre regarding attempted or actual telemarketing fraud.*

[11] *"Criminal Misuse of Internet: Policing Challenge of 21st Century", Press statement quoting Albert Pacey, Director General of the NCIS, May 28, 1997.*

- Cases that respond to emerging new threats and risks, in order to slow the spread of new criminal approaches and ensure the Force stays "ahead of the game. (Most stakeholders expect that there is a substantial overlap between these three types of cases.)

- Providing leadership and coordination, through the development of a stronger intelligence capability and the sharing of information with relevant stakeholders, leading to a more proactive approach to combating economic crime. This leadership approach does not preclude partnership arrangements, which are necessary to exploit the differing strengths of each of the participants/

This means that its officers should have the level of training to carry out these more challenging cases, and that continuity (e.g., maintenance of a consistent level of skill and experience) and consistency of approaches across the country needs to be established and maintained.

IV

Assessment Of The Program's Mandate And Associated National Interest And International Harmonization Issues

---

This chapter reviews two aspects of the mandate of the Economic Crime Program: the scope of the mandate as currently defined, and the structure of the "national interest standard" which forms part of the mandate. Our analysis and conclusions on the mandate then directly relate to the fourth primary objective for this study – *To clearly define what is meant by the "national role and interests" of the Economic Crime Program* (PO4).

The chapter then goes on to examine two other objectives for the study, which are linked to the mandate and national interest standard:

- *To devise a methodology for determining the relative benefits gained by the key players, at the federal and provincial levels, and, hence, a means of allocating more accurate costs of the program amongst its participants.* (PO2)
- *To recommend the extent to which Canada and the U.S. must harmonize their enforcement efforts to carry out related responsibilities in the field of economic crime.* (PO5)

A. Clarity and focus of the Program's mandate needs to be sharpened

Establishing a clear mandate for the Economic Crime Program is vital to determining the level and mix of required resources for the Program. The mandate defines the scope and focus of the work activities to be undertaken and the nature of the outcomes to be achieved using the resources allocated to the Program. Today's fiscal realities dictate that the RCMP cannot accept every request for assistance received from the public, private industry or other stakeholders. Setting a clear mandate, therefore, provides a basis for establishing ground-rules which can aid the Program's managers and investigators across the country in making consistent decisions regarding caseload. A copy of the current mandate, which was released in December 1997, is presented in Appendix B to our report.

This section assesses the clarity of the mandate for the Economic Crime Program in terms of its ability to:

- Summarize desired outcomes, that is, what is to be achieved and who is to be served?
- Identify the key operating capabilities, that is, what capabilities are necessary to achieve the desired outcomes?
- Identify the key areas of focus, that is, which criminal activities and economic crime types should the Program give highest priority to?

Our conclusions regarding the first two of these points are presented below, and the following section deals with the principal areas of focus, as part of the analysis of the "national role and interests". Exhibit IV-1 summarizes our overall approach to assessing the mandate plus recommended changes and additions, shown in italic text.

1. Anticipated outcomes, not outputs, need to be clearly stated in the mandate

Expected outputs from the Program predominate in the current version of the mandate with few or no references to outcomes or impacts to be achieved. An implication of this is that investigations are the "be all and end all" of the Program. It is important to go beyond this and also define what the Program is trying to achieve through this effort.

Our view, based on the inputs received from stakeholders and Program members, is that there are three key outcomes that it can contribute to:

1. ***Deterrence*** of perpetrators and potential perpetrators, and ***prevention*** of economic crime activities, particularly those linked to crime trends of greatest concern to police agencies, enabling business organizations, regulatory agencies and justice officials around the world, and ***dismantling of organized crime***. For example, the preceding two chapters identified a range of challenges characterized by an environment in which economic crimes are increasingly national or international in nature; criminals are using advanced computer technologies to facilitate their work; and, organized crime groups are increasing their involvement.
2. ***Prosecution and conviction*** of offenders, based upon efficient, timely and effective investigations.
3. Maintenance of a high level of ***integrity*** and ***public confidence*** in Canada's economic infrastructure. Public confidence includes not only the confidence of members of the Canadian public but also the confidence of domestic and international investors and consumers.

Exhibit IV-1
Recommended structure and core content of the Program mandate

Key mandate questions

✔ ***What key capabilities are most necessary?***

X

➪ ***What types of crime & criminal activities are focused on, as a matter of first priority?***

=

✦ ***Who does the Program serve?***

✦ ***To achieve what ends? (What is success?)***

Summary – Recommended Economic Crime Mandate

Capabilities in:

- ✔ *Intelligence gathering and dissemination*
- ✔ *Partnerships with key stakeholders in Canada*
- ✔ Investigations
- ✔ *Maintenance of specialist technical support capabilities*
- ✔ Assistance to, and cooperation with, international law enforcement agencies.

X

Focus on:

- ➪ Cases that satisfy the National Interest Standard

and involve either:

- ➪ Criminal activities related to federal statutes and programs.
- ➪ Corruption
- ➪ Commercial fraud
- ➪ Securities fraud
- ➪ Counterfeiting
- ➪ Computer crime
- ➪ Technical support for investigation of computer-assisted economic crimes.

=

In order to:

- ✦ *Deter and prevent economic crime activities.*
- ✦ *Dismantle organized crime.*
- ✦ *Prosecute and convict offenders, based on efficient, timely and effective investigations.*
- ✦ *Contribute to the maintenance of public confidence in Canada's national economic infrastructure.*

For benefit of:

- ✦ Canadians
- ✦ Government of Canada
- ✦ *Providers of national economic infrastructure*
- ✦ *Domestic and international law enforcement agencies.*

2. Key stakeholders served by the Program also need to be identified

In addition, the current mandate does not explicitly identify who it serves, other than an opening reference to responding *"to economic crime where the interests of the Government of Canada and Canadians are at stake"*. While this is correct it would be useful to be more explicit in identifying the range of beneficiaries of the Program. We see a need to identify four key stakeholders in the mandate:

1. ***The Government of Canada***, which is both a direct beneficiary, through the work of the Program on Federal Statutes and Programs, and indirectly, through its work to combat economic crime and maintain the integrity of Canada's economic infrastructure.

2. ***The Canadian public***, which benefits directly, as consumers and investors, from the Program's efforts to maintain fair and transparent commercial practices and indirectly, from the resulting contributions of these practices to the integrity of the economic infrastructure.

3. ***Public and private organizations that provide the elements of the economic infrastructure*** that enable business transactions to take place, or regulate the functioning of related markets. These organizations benefit from the Program's efforts to prevent criminal involvement in, and threats to, the functioning of the infrastructure.

4. ***International and other domestic law enforcement agencies***, which receive a range of benefits. International agencies benefit from reciprocal arrangements to combat international criminal activities, and domestic agencies benefit from a combination of access to national and international reach and/or capabilities to undertake more complex and demanding assignments.

3. Investigations are central to the Program's operations, but supporting capabilities need to be highlighted

Investigations are central to the Program's operations and, as such, dominate the current mandate definition. But not all resources, and not all effort, is focused on the conduct of investigations. These complementary and/or supporting capabilities also need to be highlighted. We see a need to refer to capabilities in:

1. ***Intelligence gathering and dissemination***. Intelligence gathering – relating to such areas as the identification, tracking and targeting of crime groups, analysis of various crime techniques, monitoring of trends in different types of crime – has been identified by many law enforcement agencies as a key way to keep "ahead of the game". As such, it needs to be explicitly identified in the mandate.

2. ***Partnerships with key stakeholders***, particularly enabling business and public organizations and sector regulatory agencies. Feedback from these stakeholders shows a strong desire to develop arrangements to enable stakeholders and the RCMP to act in a coordinated manner and maximize the impacts achieved by each. Partnerships are also critical to the intelligence gathering and dissemination function.

3. ***Investigations of alleged criminal activities***, as the basic modus operandi for the Program.

4. ***Maintenance of specialist technical support capabilities***, to undertake particular types of investigations (e.g., computer crime cases), to support the investigation of crimes involving the use of computers as facilitating tools (computer-assisted economic crimes), and to manage the selection and conduct of large, complex investigations.

5. ***Assistance to, and cooperation with, international law enforcement agencies***. While this may seem like a given, it is important to recognize that the management of international cooperation activities – at a Program-wide level and in relation to specific investigations – requires particular skills and resources.

B. "National interest" in law enforcement focuses on public confidence in, and the integrity of, the national economic infrastructure

The selection of key areas of focus in the Program mandate should be largely determined by the answer to the question: *"what is meant by the 'national role and interests' of the Economic Crime Program?"* (From PO4.) In order to answer this question three component questions need to be addressed:

1. What is the national interest in the context of economic crime?
2. What economic crime activities are most closely linked to the national interest?
3. What criteria should the Program use in its "national interest standard"?

1. What is the national interest in the context of economic crime?

Most analyses of the wider implications and issues regarding economic crime make only passing reference to the "national interest" and few provide precise definitions. Our own view, and drawing upon the available information[12], is that the national interest in law enforcement relates to:

- ***Protection of the integrity of the national economic infrastructure***, which involves both private and public sector infrastructure providers.
- ***Maintenance of public confidence in the integrity and safety of the economic infrastructure***, spanning its component market structures and transaction systems, as well as the integrity and equity of federal revenue (e.g., tax collection) and social (e.g., Employment Insurance) programs. Public

---

[12] *These views largely draw upon a definition of the Commonwealth of Australia's interests in law enforcement, as defined in the Australian Federal Police Act 1979 and a subsequent review study – the Review of Commonwealth Law Enforcement Arrangements – undertaken in 1994.*

confidence, in this sense, relates to the confidence of the Canadian public generally and in the public's roles as consumers and investors, plus the confidence of international customers and investors.

- ***Maintenance of public confidence in the integrity of public management and political oversight of the functioning of government.***
- ***Maintenance of a flexible and competitive economy***, such that law enforcement requirements are balanced against needs for commercial responsiveness and competitiveness.
- ***Efficient resource management to optimize expenditures on law enforcement*** across all jurisdictions and types of stakeholders (law enforcement agencies, regulatory agencies and enabling business and public service providers).
- ***Consistent approaches to law enforcement*** involving economic crime incidents across Canada.

The first three elements of the national interest relate to outcomes that law enforcement should contribute to in conjunction with other government policies and programs. The final three elements relate to the efficiency and effectiveness of law enforcement operations.

No single agency or organization acting in isolation can expect to ensure that the national interest is satisfied or maintained. The Economic Crime Program has a key role to play, acting in cooperation with regulatory agencies and enabling business and public service providers as well as international law enforcement authorities.

2. What economic crime activities are most closely linked to the national interest?

Potentially, all types of economic crime can have a bearing on the maintenance of the national interest. Some may have a greater impact on the integrity of the national economic infrastructure (e.g., payment card or securities fraud) than on the integrity of public sector management and political oversight than others (e.g., fraud or corruption under federal statutes and programs), but all have the potential to weaken public confidence if they are largely ignored by law enforcement agencies.

The issue then, is not what types of crime affect the national interest and thus fall within the mandate of the Program, but which types of criminal activities should fall within the mandate.

Crimes committed against federal programs may be an exception in that they are a type of crime that falls directly under the mandate of the RCMP. However, this should not prevent the RCMP from working with the affected departments to find more cost-effective ways to address some of the types of criminal activity that are going on, especially if time or resource savings can be achieved while limiting the incidence of criminal activity. For example, greater use of in-house investigatory capabilities or services contracted from private sector sources, such as forensic accountants, as well as greater use of administrative and civil penalties and controls may be a more cost-effective route to pursue in many instances.

In our interviews, stakeholders consistently identified a range of activities that they believed the Program was best able to undertake, and thus could be expected to make a significant contribution to the maintenance of the national interest:

- Investigation of cases that:
  - Involve organized crime groups that account for significant losses or disruption.
  - Involve large scale, systemic fraud, computer crime or other types of economic crime.
  - Have regional, national and/or international dimensions.
  - Require higher levels of expertise and specialized knowledge to investigate, due to their complexity.
  - Respond to emerging threats and risks.

  (Note that these aspects need not be mutually exclusive.)
- Intelligence collection, analysis and dissemination.

The next section considers how these activities may be used to guide the selection and prioritization of cases and other activities.

3. What criteria are needed in the "national interest standard"?

Many special purpose police units incorporate criteria in their mandates to guide the selection and prioritization of their investigations. Examples include those of the U.K.'s Serious Fraud Office and the Australian Federal Police, which are summarized in Exhibit IV-2.

Exhibit IV-2
Case selection criteria used by other law enforcement agencies

Australian Federal Police – Prioritisation of Referrals

AFP has a series of factors, in two categories, to be considered when determining the priority to be allocated to all referrals or tasks requiring the commitment of AFP resources.

Essential

Any tasks falling into this category must be accommodated by the AFP. Policy, strategic or operational issues that arise as a result are addressed by a National Priorities Group (comprised of senior officers, including the Commissioner). Factors to be considered are:

- Specific referral by the government.
- Criminality and impact of the crime.
- High political impact or sensitivity.
- Direction from the AFP National Priorities Group.
- Treaty obligations and agreements (e.g., assistance to international agencies).

Very Important

These factors provide guidance in determining the "value" of undertaking various tasks and hence a way of determining importance relative to other tasks or referrals, and relate to:

- Need for timely response.
- Priority relative to existing tasks.
- Deterrence value.
- Appropriateness of AFP involvement (e.g., is jurisdiction clear, would administrative or civil remedies be better, does the AFP have the necessary skills, should another agency lead (with AFP support), etc.)
- (Potential for) significant return to the Commonwealth.
- Resource intensity.
- Intelligence value.
- Training and development value.
- Probability of a successful outcome.
- (Potential to) strengthen national and international cooperative arrangements.
- (Potential to establish a) new strategic direction for AFP.
- (Need for) consistent AFP approach (e.g., AFP may have undertaken a similar task or referral in the past).
- Strategic alliance (e.g., subject to an existing agreement or MOU with another agency).

Exhibit IV-2 (cont'd)
Case selection and prioritization criteria

Serious Fraud Office – criteria for accepting cases

The key criterion for deciding whether the SFO should accept a case is that the suspected fraud is such that the direction of the investigation should be in the hands of those responsible for the prosecution.

Certain additional factors are also taken into account, relating to the characteristics of proposed cases:

- Monies at risk or lost are at least £1 million (as a signpost of seriousness and likely public concern, rather than the main indicator of suitability).
- Likely to give rise to national publicity and widespread public concern.
- Requiring highly specialized knowledge.
- Significant international dimension.
- Legal, accountancy, and investigative skills need to be brought together.
- Appear to be complex, and in which the use of Section 2 powers may be appropriate (mandatory for persons being investigated to furnish information and produce specified documents).

None of these factors, taken individually, should necessarily be regarded as conclusive.

The Program's current mandate includes a "national interest standard" that shares some of the characteristics of the two examples provided in Exhibit IV-2. However, we believe a number of changes are required to ensure it provides direction to the Program to ensure it contributes to the maintenance of the national interest. Accordingly, we recommend the incorporation of a revised "national interest standard" in the Program mandate, as shown in Exhibit IV-3.

Examination of the criteria presented in Exhibit IV-3 shows:

- A primary focus on cases that are more complex and extensive, require a high level of expertise to investigate, involve organized crime groups and which may generate widespread public and/or political concern. This means that a significant proportion of cases taken on will fall into MIS Classes 2 and 3.

- Additionally, or alternatively, cases that indicate the emergence of a new criminal approach or risk should be undertaken as a matter of priority, as should cases that provide opportunities to create a significant deterrence effect or where there are no effective civil or administrative sanctions available.

Exhibit IV-3
Recommended "national interest standard" for the Program

The Economic Crime Program undertakes investigations, and related activities, in which one or more of the following factors are present:

- ☐ Involvement of organized crime group(s).
- ☐ Large scale systemic fraud, involving a large number of victims and/or a significant financial risks or losses.
- ☐ Complex:
  - Involving a high degree of criminal sophistication;
  - Requiring a high degree of investigative and/or technical expertise; and
  - National or international in scope.
- ☐ Widespread (regional, national or international) public concern or interest in combination with political interest or the potential thereof.
- ☐ Emergence of an apparent new risk or criminal approach, with potential for rapid diffusion, or significant financial risks or losses, if left unattended.
- ☐ Opportunity to achieve a strong deterrence effect, either by sending a message to criminal groups or encouraging greater caution on the part of consumers and/or investors.
- ☐ No scope for administrative penalties of civil actions, or such approaches are proving to be ineffective.
- ☐ Action required under the terms of an existing treaty, agreement or memorandum of understanding with other law enforcement agencies, regulatory agencies or industry groups representing the interests of enabling business organizations within the economic sector targeted by the criminal activity.

A "Program and case priorities group" composed of a small number of senior Program managers (e.g. Director, officer(s) in charge of various crime groups and regional managers) is also desirable, to resolve questions regarding the assessment of certain cases and to regularly review the working of the national interest standard and results achieved by the Program.

- A probable need to appoint a "Program and case priorities group" to resolve issues relating to the selection of cases for investigation (because there will always be anomalous situations occurring), to regularly assess results achieved against the mandate commitments and determine if the mandate is continuing to keep abreast of the expectations set for the Program by RCMP senior management and/or its Minister.

Equally important is the issue of what happens to cases that do not satisfy the Program's national interest standard. These cases should either be undertaken by provincial police services (RCMP commercial crime units or General Investigative Sections (GIS) in provinces where the RCMP provides contract police services) or municipal police services. The expectation of the national interest standard is that those cases that are not investigated by the Program can be handled within the resources and capabilities of complementary law enforcement agencies. Additionally, a proportion of cases may be suited to the pursuit of administrative penalties or civil remedies, necessitating arrangements with these organizations to ensure that such cases do not "fall through the cracks".

We have not made "substantive value" a criterion in its own right. The focus of stakeholder expectations and the maintenance of the national interest in law enforcement is more on the issues of public confidence and integrity of the economic infrastructure, which require the pursuit of cases with a range of values to maximize deterrence impacts. Public confidence and integrity of the economic infrastructure will often be associated with cases involving significant losses or risks of losses, but not always. Additionally, the Program's own file records show that there is no correlation between estimated file values and the amount of time (and presumably complexity) required to bring a case to fruition.

Given these points, we see a need for the mandate to continue to cover the following areas of economic crime:

- Commercial fraud, including telemarketing and Internet fraud
- Securities fraud
- Payment card fraud
- Counterfeit currency
- Computer crime (unauthorized access and mischief to data)
- Theft of telecommunications
- Federal Statutes and Programs, spanning bankruptcy investigations, economic crimes where the Government of Canada is the victim such as fraud, corruption and financial theft, and *mens rea* offences under the federal statutes listed in the current mandate (excluding the Income Tax Act, where, we understand responsibility has been transferred to IPOC).

Potentially, software theft could be added to the types of crimes covered by the Program. Software theft is characterized by the illegal copying and duplicating of software programs, most often standalone business and home/game software programs[13]. Software theft, or software piracy as it is often referred to as, is a significant crime, with an estimated value of losses (revenues foregone by software manufacturers) of approximately $360 million in Canada[14]. However, it probably does not have the same potential to damage the overall integrity of, and public confidence in, the national economic infrastructure in the same way that, say, computer crime could.

We recommend that the "Program and case priorities group" look at the characteristics of software piracy in more depth and determine, in consultation with their colleagues in other RCMP units, whether software piracy fits most appropriately under the Program's mandate, as an extension of computer crime.

C. Determination of relative benefits gained by key players

The second primary objective for our work was to *devise a methodology for determining the relative benefits gained by the key players, at the federal and provincial levels, and, hence, a means of allocating more accurate costs of the program amongst its participants.* Two interpretations of "benefits" are possible in this context:

- How do the key players benefit from the work of the Program's officers and can these benefits be disaggregated to show a benefit to each?
- How do the federal and provincial levels benefit from the current arrangements for providing both federal and provincial economic crime positions in provinces with contract arrangements (i.e., all provinces except for Ontario and Quebec), and are these benefits in line with the current cost sharing arrangements and resource allocations?

After careful review of the findings from our interviews and supporting analysis we have concluded that it is not possible to separately measure the benefits that flow to each of the key players and thus cannot base an allocation methodology on this approach. However, it is possible to obtain indicative comparisons on the second interpretation of "benefits" that compare current numbers of federal and provincial positions to estimates of requirements based on the population per position in Ontario and Quebec. We recommend that this approach be used as an aid to analysis and planning for contract negotiations, not as a definitive methodology as the underlying assumptions have a number of significant limitations.

---

[13] *See, for example, "Software piracy easy, prolific and too well accepted by Canadians",* ***Silicon Valley North****, Ottawa, May 1998,*

[14] ***1996 BSA/SPA Piracy Study Results****, Prepared by the U.S.-based Business Software Alliance (BSA) and Software Publishers Association (SPA), May 1997. (www.spa.org/piracy/releases/96tables.htm)*

The following sections summarize the findings on these two lines of analysis and present our recommendations for the Program's approach to future negotiations with the contracting provinces.

1. Federal and provincial governments are key players but the public and enabling organizations do not, or cannot, differentiate between federal and provincial benefits

As a first step, it is important to identify who the key beneficiaries are and the benefits they are seeking to achieve. Each of the primary stakeholders (as identified in Chapter III), plus the federal and provincial governments acting in their overall policy setting and funding roles, expects to realize a number of benefits. We have summarized our assessment of these expected types of benefits in Exhibit IV-4.

Examination of this summary shows that:

- Maintenance of the integrity of, and public confidence in, various elements of the economic infrastructure are benefits that are sought by both federal and provincial governments, as well as private and public organizations that physically provide and maintain these elements.
- Members of the public have a similar benefits expectation, in so far as their confidence in the infrastructure depends upon the maintenance of safe, secure and transparent commercial/administrative practices and systems.
- The benefits described in Exhibit IV-4 are public goods. The public good from law enforcement that we realize as citizens of Canada is inseparable from the public good we realize as citizens of a particular province; that is, the benefits are seen as being one and the same for each level. The trend towards global business networks and markets further reinforces this seamless perception of benefits.

Exhibit IV-4
Key players and expected benefits from economic crime policing

Stakeholder Organizations	Expected Benefits from the Program's Policing Activities
Members of the Public	• Safe, secure and transparent commercial/administrative practices and systems. • Confidence in, and willingness to use, elements of the economic infrastructure without disruption or damage to individual "economic identities". • Protection of assets and savings.
Enabling Business and Public Organizations	• Minimization of losses to, and disruption and damage from, economic crimes. • Maintenance of competitiveness and attractiveness to investors (including the federal government as the funding 'shareholder' for public sector service providers). • Public confidence in the integrity of products, services and systems.
Regulatory Agencies	• Contribution to minimizing the incidence of economic crimes, via impact of prevention, deterrence and prosecution of criminal activities. • Contribution to maintaining fair, transparent and efficient markets. • Public confidence in the integrity of markets and frameworks for consumer protection.
Federal Government	• Minimization of losses to, and disruption and damage from, economic crimes committed against federal departments. • Maintenance of Canada's positive image as a place to invest and do business, based on protection of the integrity of the economic infrastructure and maintenance of public confidence. • Maintenance of the integrity and fairness of revenue collection and social programs, leading to optimal value for taxpayers. • Optimal expenditure levels, and value-for-money, for law enforcement.
Provincial Governments	• Maintenance of the integrity of provincial economic infrastructure, as an integral component of the national economic infrastructure. • Maintenance of public confidence in the components of this infrastructure. • Minimization of losses to, and disruption and damage from, economic crimes committed against provincial departments, which may be committed from within the province, or from another province or internationally.

2. Sources of benefits to provincial governments can be described, but not quantified

Actions by the Economic Crime Program to combat criminal activities produce a mix of benefits that can be expected to reduce the incidence or magnitude of economic crimes within each province, compared to rates that would likely be experienced if provinces had to rely on standalone "provincial economic crime programs". We see these benefits arising in the following ways:

- Actions taken to combat economic crime outside of the federal statutes and programs area are likely to reduce provincial rates of economic crime in two areas:
  - Direct impacts and benefits produced when the Program targets crimes committed and/or crime groups based within a particular province, leading to reduced risks to consumers and investors, and improved integrity of the economic infrastructure.
  - Indirect, or flow-on, benefits resulting from Program actions in other provinces or internationally that may prevent losses to consumers resident within the province in question and/or send a strong deterrence message to local economic crime groups.
- Actions taken in relation to federal statutes and programs that are directed towards satisfying the needs of federal government departments and agencies may also produce benefits at the provincial level. For example, if cases of criminal tax avoidance are targeted and the integrity of tax programs is strengthened, then provincial tax receipts will also benefit (due to tax sharing commitments). Similarly, actions targeting federal social programs, such as EI fraud, may also deter fraud related to provincial health and welfare programs.
- In addition, the overall effectiveness and efficiency of policing can be improved if provincial (and municipal) programs targeting economic crime complement the federal program and priorities. In particular, a critical mass can be established to develop and enhance specialized skills that can be deployed on a national basis, interprovincial and international crime investigations can be more readily undertaken, the gathering and use of criminal intelligence can be approached on a national basis, and consistent national approaches and standards can be applied in conjunction with national stakeholders and partners.

From this perspective, provincial governments are able to obtain a higher value (and lower cost) policing service if provincial policing programs targeting economic crime complement the federal Program. However, while these qualitative benefits are readily apparent it is not possible to separate and measure the proportion of the Program's operations and activities that provide "provincial benefits" and that which provides "federal benefits", on this basis.

3. Current allocations of federal and provincial positions in a number of contract provinces may be out of line with needs and funding structures

The key issue concerning the current arrangements for provincial funding of positions within the Economic Crime Program in contract policing provinces, and the associated balance between designated federal and provincial positions, is the belief that these arrangements favour the provincial governments. In other words, the provinces are believed to be getting a "free ride", and thus undue benefits, at the expense of the federal positions and program funding.

One way of testing this belief is to use the two provinces that do not have contract policing arrangements with the RCMP – Ontario and Quebec – as a benchmark for estimating what the allocation between federal and provincial positions should be if the decisions as to federal and provincial resource levels were being made independently.

The hypothesis here is that, if a contract policing province is getting a "free ride" it will have fewer provincial positions than would be the case if the provincial and federal programs were in separate organizations (as is the case in Ontario and Quebec). In such a situation one would expect that either the total number of economic crime positions in the province would be below the level suggested by the benchmarks or that other levels of government – federal and/or municipal – would have a larger number of dedicated positions than would otherwise be the case (i.e., would have "taken up the slack").

However, this approach rests on a number of significant assumptions that mean that it can, at best, provide only a general indication as to whether any of the contract provinces are receiving undue advantages from their arrangements with the RCMP for economic crime investigations. These assumptions, and the estimates obtained using the approach, are presented in the following sections.

a) Limitations of the key assumptions cannot be ignored

In using the comparative benchmarking approach outlined above we are making three key assumptions:

1. **Distinct mandates and separate areas of focus for federal, provincial and municipal economic crime units.** If we use the Ontario and Quebec provincial unit sizes without consideration of the existing federal and municipal police roles we are assuming that there is no overlap, or substitutability, between the roles of the respective economic crime units. However, a comparison of the mandates of the OPP's Anti-Rackets Section and the Toronto Police Service's Fraud Squad shows a significant amount of overlap and, in turn, both overlap with the mandate of the RCMP Program. This means that many investigations could be undertaken by either the RCMP, a provincial unit or a municipal unit.

   Given this fact, it is necessary to also include the federal and municipal economic crime units in the analysis to obtain an estimate of overall resource levels and an indication of the "ideal" balance that may be desirable between federal, provincial and municipal units dedicated to fighting economic crime.

2. **Optimal resource levels in the Ontario and Quebec units.** The approach implicitly assumes that Ontario and Quebec have an optimal number of investigators in their economic crime units. We were not able to verify this assumption; however, comments made by representatives of some of the provincial and municipal units during our stakeholder consultations suggest that these units are facing the same resource limitations and funding constraints that are being experienced by the RCMP Program. This means that any estimates of required resource levels based on the combined Ontario and Quebec benchmarks should probably be viewed as a minimum, or as indicative only.

3. **Population figures provide a reasonable proxy of relative levels of economic crime.** If our estimates are based on population per force member we are assuming that the level of economic crime is highly correlated with the size of the population. We believe that there is a correlation but that other factors will work to diminish the significance of this correlation. In particular, the advent of the Internet, seamless international telecommunications networks, and global financial markets mean that the incidence and impacts of many types of economic crimes need not be linked to the size of the population in a particular city or province.

As we have noted, the weakness of the first assumption can be overcome to a certain extent by using data on the number of federal, provincial and municipal economic crime officers rather than working with provincial numbers alone. As to the other two assumptions, work could be undertaken to establish what the optimal resource levels could be for the economic crime units in the Ontario and Quebec provincial police forces, and to clarify the correlation between economic crime rates, population and other socio-economic factors. Such work goes well beyond the scope of our current work and would require extensive research. Given this, it must be accepted that the comparative benchmarking approach provides indicative answers only.

b) Application of the benchmarks suggests the federal-provincial balance is out of line in some provinces

Exhibit IV-5 summarizes the benchmarks calculated using the combined population of Ontario and Quebec and information on the number of police positions in the federal, provincial and municipal economic crime units. Data was collected from the RCMP, Ontario Provincial Police, Sureté du Quebec and the major Ontario regional police forces. Only municipal forces with units dedicated to economic crime investigations were included in the calculation of benchmarks.

Examination of the data in Exhibit IV-5 shows a high degree of similarity between the two provinces in terms of the number of people per federal position, per provincial position and for all (federal, provincial and municipal) positions. The number of people per municipal position differed more markedly between the two provinces, which may be a function of using the provincial population as a basis for estimating requirements within major municipal areas.

Exhibit IV-5
Relative scale of economic crime investigation capacity in Ontario and Quebec

	Ontario	Quebec	*Combined*
Federal Positions (RCMP)	127	92	219
Provincial Economic Crime Units	79 (OPP)	52 (SQ)	131
Municipal Economic Crime Units	55 (Toronto) 15 (Ottawa-Carleton) 22 (Peel) 8 (Hamilton-Wentworth)	44 (Montreal)	
	100	44	144
TOTAL -- ALL LEVELS OF GOV.	306	188	494
Est. 1997 Population (,000)	11 407.7	7 419.9	18 827.6
People/Federal Position	89 824	80 651	85 971
People/Provincial Position	144 401	142 690	143 722
People/Municipal Position	114 077	168 634	130 747
People/Prov.+ Fed. Positions	55 377	51 527	53 793
People/All Positions	37 280	39 468	38 113

Note: RCMP figures are the number of positions; Ontario is A and O Divisions.
Population figures from Statistics Canada, Cansim matrices 6367 and 6379.

Exhibit IV-6 provides estimates of the required levels of federal, provincial and municipal unit numbers, based on the benchmark indicators calculated in Exhibit IV-4, and a comparison to the current numbers of positions. The fact that both Ontario and Quebec have municipal police forces that have dedicated economic crime units presents some difficulties in applying the benchmarks in Saskatchewan, New Brunswick and PEI where there are, to our knowledge, no such units. In these provinces, the municipal estimates (9 in Saskatchewan, 7 in New Brunswick and 1 in PEI) should be considered as being equivalent to additional FTE requirements in GIS detachments deployed in the major cities in each province.

Examination of the information in Exhibit IV-6 suggests that:

- The total number of positions for all eight contract policing provinces combined is in line with that in Ontario and Quebec, that is, application of the benchmarks suggests there should be 298 positions; the current actual level is 299.
- Distinct variations occur between different provinces. British Columbia, Alberta, Saskatchewan and New Brunswick have investigator levels below the benchmark rates (also the estimates for these last two provinces may be skewed by the method of estimating provincial and municipal positions), and Manitoba and Nova Scotia have levels above the benchmark rates.
- In Alberta, provincial levels are significantly below the level estimated by the benchmark rates and that both the number of federal and provincial positions has expanded to fill this void.
- A somewhat similar position appears to hold in British Columbia, with the federal positions expanding to meet the gaps at the provincial and municipal level. (An alternative way of interpreting the results could be that provincial and municipal levels have not grown to the levels suggested as necessary by the benchmark rates because the RCMP has been persuaded to maintain higher numbers of federal positions.)
- In Nova Scotia and Manitoba, the municipal force size is well above that suggested by the benchmark rates, which may have resulted in (or enabled) a below-benchmark level in the level of federal positions in Nova Scotia (but not Manitoba).
- In the remaining provinces, the balance between federal and provincial positions is generally in line.

Exhibit IV-6
Estimated allocation of federal, provincial and municipal economic crime resources based on Ontario-Quebec benchmarks

	Population (1997)	**Estimated Numbers Based On Ontario-Quebec Benchmarks**				**Current Numbers Of Positions**			
		Federal	**Provincial**	**Municipal**	**TOTAL**	**Federal**	**Provincial**	**Municipal**	**TOTAL**
British Columbia	*3 933 300*	46	27	30	**103**	57	25	19	**101**
Alberta	*2 847 000*	33	20	22	**75**	38	7	26	**71**
Saskatchewan	*1 023 500*	12	7	8	**27**	13	9	▨	**22**
Manitoba	*1 145 200*	13	8	9	**30**	15	9	17	**41**
New Brunswick	*762 000*	9	5	6	**20**	9	4	▨	**13**
Nova Scotia	*947 900*	11	7	7	**25**	7	9	14	**30**
PEI	*137 200*	2	1	1	**4**	3	3	▨	**6**
Newfoundland	*563 600*	7	4	4	**15**	6	5	4	**15**
TOTAL	*11 359 700*	132	79	87	**298**	148	71	80	**299**

4. Potential implications of the comparative analysis and recommendations regarding the benefits methodology

Application of the combined Ontario and Quebec benchmark rates to the contract provinces suggests that both British Columbia and Alberta should have a higher number of provincial positions, and fewer federal positions. In this sense then, there is support for the view that these two provinces may be getting a "free ride" and that federal positions (and municipal positions too, in Alberta) have expanded to meet demand for economic crime investigations.

The approach used may assist the Program to determine appropriate balances between federal and provincial investigation needs, but requires further research and fine tuning to overcome the limitations identified above. As such, it does not provide a definitive methodology for determining the relative benefits gained by the key players, at the federal and provincial levels, and, hence, a clear and defensible means of allocating program costs between its participants.

Given this, we recommend that:

- Current agreements for provincial contributions to the cost of the Program should remain in place until the end of these contract terms.
- The Program should undertake a more extensive program of data collection and research to obtain a better understanding of the current balance between investigations that are essentially aimed at meeting provincial needs and those that satisfy the national interest standard or are directed towards investigations under federal statutes and programs. This task would be made easier if the Program applies its national interest standard on a rigorous and consistent basis, and moves to a national service line approach with costing and charge back arrangements for work undertaken to meet obligations under provincial contracts and to satisfy agreed service standards.
- The Program should use the information obtained from the above research to develop proposals for re-negotiating the basis for meeting provincial needs when their contracts come due, and to use the findings to support such negotiations.

D. Canada/US harmonization of enforcement efforts

This section addresses Primary Objective #5 set for the study: *To recommend the extent to which Canada and the U.S. must harmonize their enforcement efforts to carry out related responsibilities in the field of economic crime.*

In recent years, information technologies and regulatory changes have greatly accelerated the globalization of virtually all aspects of business. Tremendous progress towards internationalization has been made through multilateral trade agreements which seek to reduce or eliminate outmoded trade regulations, creating a business environment that facilitates the fair exchange of goods and services across international borders. As economic (and other) benefits derived from the establishment of international rules and standards are becoming widely recognized, the calls for further harmonization of activities across the private and public sectors are increasing.

Economic crimes and law enforcement in this area have followed this global trend. It is widely-accepted that the investigation and prosecution of white collar crimes stand to gain significant benefits from the increased international harmonization of strategies and efforts. Potential benefits include faster handling of cases, improved quality/presentation of evidence and reduced workload for both investigators and the court system.

While multilateral negotiations in this area have moved forward steadily during the 1990s, a priority for Canada remains its harmonization efforts with the United States (given the high degree of integration of our two economies).

1. Current Canada/US "disharmonies" in economic crime law enforcement

Law enforcement activities in the area of economic crime are carried out within a regional, national and international context that is shaped by social, environmental, technological and legal influences and infrastructures. These influences have historically varied from region to region, reflecting socio-economic and demographic differences, political imperatives, etc.

These systemic differences are often most-visibly manifested at the working level, whereby day-to-day decisions and actions are guided (or constrained) by legal boundaries that define how work is to be carried out. Examples of these impacts have been highlighted in the paragraphs below[15].

a) High costs

A high proportion of the cost of any investigation is driven by the number of hours of effort required by representatives of policing agencies, the legal community, the courts, etc. The workload required of RCMP investigators in certain categories of economic crime, such as telemarketing fraud, can be significantly greater than that of their American counterparts. For example, in preliminary hearings in Canada, Crown Attorneys often call for first-person testimony—e.g., necessitating multiple witnesses—to ensure formal court hearings are held .

---

[15] *It should be noted that approaches within the RCMP can vary by region, in accordance with "best practices" at adopted the local level. The examples cited below represent general observations.*

By comparison, Grand Jury hearings in the US (conducted to determine whether or not to proceed to formal trial), in many circumstances, allow for the establishment of probable cause based on the sworn testimony of the police officer. In the US, general conspiracy statutes make it a separate federal felony to conspire to commit mail fraud, telephone fraud (wire fraud), etc. Thus, law enforcement investigators need only establish that a group of people is taking concerted action to bring to fruition the conspiracy to commit an offence in this area. As a result, the existence of a federal crime can be established based on summary evidence and testimony of how a scheme was put together (without calling together most or all of the victims to testify on the stand).

Similarly, "dollar-for-dollar" proof (again necessitating that each victim be called to testify in person) in fraud cases has often been required in Canada to obtain the conviction. When applied to a telemarketing fraud case involving transporting hundreds of elderly victims (who cannot travel or must come from long distances), the potential costs and logistics become daunting.

By contrast, under similar circumstances, US law might require that only 10 cases of fraud be proved to demonstrate guilt, allowing the magnitude and subsequent sentencing to be determined afterwards through statistical analysis and scrutiny of bank transaction records, interview notes, etc.

Another example of the additional workload in Canada brought to bear by other legal/technical limitations is the requirement of formal court authorization of wiretapping. In the US, provisions are more lenient and in many lower-risk situations (e.g., consensual monitoring by police of victims' telephone lines), formal court approval is not required.

b) Lengthy time delays

The current legal process is widely-perceived to be slow and cumbersome, not only due to a burgeoning backlog of cases, but also as a result of legal provisions put in place over the years to respond to the challenges of handling more traditional types of crime. At that time, few could have envisaged the potential scope and magnitude of the technology-assisted, cross-border organized economic crimes of the 1990s.

Delays in shutting down a fraud operation invariably result in higher numbers of victims and increased costs of investigations and prosecutions. Lengthy delays can increase the difficulty of gathering evidences, as offenders typically move to new locations.

Systemic factors which may make the investigation and subsequent prosecution of certain crime types (e.g., cross-border, white collar) inherently less appealing for prosecutors become, by extension, inherently more appealing for organized crime. Knowing how to take advantage of these systemic deficiencies can enable organized crime elements to set up, run and subsequently close down a blitz operation (such as a telemarketing "boiler-room") in a given jurisdiction before police agencies can mobilize to build a sufficiently strong case for arrest and/or prosecution.

Working across international borders further compounds the challenges faced by law enforcement teams. While Canada/US Mutual Legal Assistance Treaties (MLATs) and extradition treaties have established a formal framework for the gathering and sharing of court-admissible evidence, resource constraints within the police agencies and the courts can lead to these cases being given lower priority than priority cases from within one's own jurisdiction. The net result is that the need for recourse to MLAT provisions can easily add one or more years to the duration of a typical case. Significant additional delays can also occur if the accused criminals employ multiple appeals (e.g., a criminal could challenge the transfer of evidence to another jurisdiction well before charges have been filed).

c) Uneven results

Measuring the quality and success of Canada's policing and legal systems extends beyond basic performance indicators for criminal investigations, such as numbers of arrests and/or convictions. Maintaining public security also involves crime-prevention through public education and maintaining a strong "veil of deterrence", by increasing the probability of being caught and/or the severity of the consequences (to dissuade would-be criminals from acting). Strong proceeds-of-crime provisions also help reduce the profit potential of such crimes.

Many investigators and stakeholders interviewed felt that Canada currently lacks legislation with appropriate punitive penalties, which causes to a ripple effect throughout the legal system:

> *"If white collar criminals are not given stiff sentences including time in jail, such as 18 months to two years for first offence and 10-15 years for running full-scale operations, then the prosecutors won't prosecute. In turn, investigators can't take a case to the prosecutors if it will end up going nowhere."*

Known weaknesses in the policing or legal system can be exploited by the criminal element who choose to "play the odds", targeting specific geographic locations where the risk of detection, arrest and/or prosecution is felt to be minimal. Police raids on unscrupulous telemarketing operations, for example, have uncovered "Do not call" lists, identifying states or provinces having the strongest law enforcement teams or the most stringent laws.

Making a given jurisdiction less attractive to criminals requires the concerted effort of both police forces (through adequate investigator training and resourcing) and the legal system (through changes to legislation, court procedures and sentencing provisions) in order to close down perceived "safe havens" across North America as well as abroad.

2. Canada/US harmonization initiatives

Most stakeholders in the area of economic crime law enforcement concur that increased Canada/US harmonization of strategies and efforts will yield significant benefits on both sides of the border. Harmonization is a complex and long-term process, however, and achieving the desired benefits will require ongoing bilateral talks at the agency, regional and national level to address simultaneous changes on a variety of fronts. Many such efforts are already underway within a limited context, yet in most cases their recommendations can be expanded to apply equally to economic crime as a whole. For example, the 1997 Canada/US Working Group on Telemarketing Fraud represents the first joint effort to develop a bi-national approach to addressing telephone fraud through the sharing experiences and the establishment of institutional relations across all levels of government.

Other recent initiatives have included regulatory and law enforcement efforts having an agency-specific or regional focus—initiatives which could be replicated successfully at the international level. Furthermore, changes to provisions of the Competition Bureau Act and the Extradition Act in Canada are seeking to provide new avenues for ensuring justice can be served in serious cases of economic crime.

Representatives at the 1998 Birmingham Summit have reiterated that an effective law enforcement response to the problem of economic crime is dependent on increased international cooperation, and have restated their support for the steps undertaken by the G8 Lyon Group to implement the 40 Recommendations on transnational crime (refer to Appendix F). Canada/US harmonization initiatives are in line with these recommendations and are breaking new ground in terms of forging cooperative bilateral relationships. The US Attorney General is focusing at present on two priority areas: 1) how to get information/evidence across the border (both ways), and 2) how to get people across the border (both ways).

Exhibit IV-7 highlights a number of additional examples of proposed harmonization initiatives, many of which are currently underway. For presentation purposes, these have been grouped into four categories, reflecting the legal, environmental, technological and social influences/infrastructures which must be addressed simultaneously to maximize the effectiveness of harmonization efforts.

Exhibit IV-7
Examples of current or proposed Canada/US harmonization initiatives

LEGAL: introducing amendments to statutes and policies which address the challenges brought to bear during the 1990s through the advent of high technology-assisted forms of economic crime

- Put in place legislation with appropriate punitive penalties to serve a as strong deterrent for economic crime; Establish standard sentencing guidelines for certain categories of economic crime (e.g., a "point system" for telemarketing based on number of victims, number of operating locations, etc.).
- Review current Canada/US MLAT and extradition treaties to determine their applicability in the context of economic crime in the 1990s (e.g., amendments to the Extradition Act to streamline appeal processes). Explore the possibility of expanding MLAT provisions and of developing "fast-track" procedures for investigating and prosecuting straightforward, lower-risk cases of transborder crimes.
- Explore means of disrupting crimes by reducing the freedom of access of offenders to the telecommunications links they require to conduct illegal activities. (For example, the current requirement in Canada is that a suspected telemarketing fraud operator be convicted before telephone access can be blocked. This potentially enables them to continue fraudulent operations while awaiting trial.)
- Pursue amendments to the Canada Evidence Act (e.g., allow allowing for testimony via remote teleconferencing), as well as to cross-border search and seizure mechanisms for gathering electronic evidence that are currently available to investigators.
- Require financial institutions to establish mechanisms to monitor suspicious electronic transactions and to trace these electronic transfers to provide assistance to law enforcement agencies.
- Review the possibility of deporting foreign nationals caught engaging in economic crimes and alert law enforcement agencies as to cases when such recourse may be possible.

ENVIRONMENTAL: ensuring effective approaches and mechanisms for crime prevention, law enforcement and punishment are used consistently in jurisdictions across North America

- Coordinate investigation/prosecution strategies at the agency, regional and national level, focusing on three parallel elements: **enforcement** (e.g., rapid responses, sharing of expertise and "best practices" to improve success rates); **punishment** (e.g., deterrence through strong sentencing and public awareness of the consequences; **prevention** (e.g., public awareness to warn potential victims and reduce the profitability of scams).

12

Exhibit IV-7
Examples of current or proposed Canada/US harmonization initiatives

LEGAL: introducing amendments to statutes and policies which address the challenges brought to bear during the 1990s through the advent of high technology-assisted forms of economic crime

- Put in place legislation with appropriate punitive penalties to serve a as strong deterrent for economic crime; Establish standard sentencing guidelines for certain categories of economic crime (e.g., a "point system" for telemarketing based on number of victims, number of operating locations, etc.).
- Review current Canada/US MLAT and extradition treaties to determine their applicability in the context of economic crime in the 1990s (e.g., amendments to the Extradition Act to streamline appeal processes). Explore the possibility of expanding MLAT provisions and of developing "fast-track" procedures for investigating and prosecuting straightforward, lower-risk cases of transborder crimes.
- Explore means of disrupting crimes by reducing the freedom of access of offenders to the telecommunications links they require to conduct illegal activities. (For example, the current requirement in Canada is that a suspected telemarketing fraud operator be convicted before telephone access can be blocked. This potentially enables them to continue fraudulent operations while awaiting trial.)
- Pursue amendments to the Canada Evidence Act (e.g., allow allowing for testimony via remote teleconferencing), as well as to cross-border search and seizure mechanisms for gathering electronic evidence that are currently available to investigators.
- Require financial institutions to establish mechanisms to monitor suspicious electronic transactions and to trace these electronic transfers to provide assistance to law enforcement agencies.
- Review the possibility of deporting foreign nationals caught engaging in economic crimes and alert law enforcement agencies as to cases when such recourse may be possible.

ENVIRONMENTAL: ensuring effective approaches and mechanisms for crime prevention, law enforcement and punishment are used consistently in jurisdictions across North America

- Coordinate investigation/prosecution strategies at the agency, regional and national level, focusing on three parallel elements: **enforcement** (e.g., rapid responses, sharing of expertise and "best practices" to improve success rates); **punishment** (e.g., deterrence through strong sentencing and public awareness of the consequences; **prevention** (e.g., public awareness to warn potential victims and reduce the profitability of scams).

Exhibit IV-7 (cont'd)
Examples of current or proposed Canada/US harmonization initiatives

- Conduct multi-disciplinary reviews of typical end-to-end process steps involved in investigating and processing various categories of economic crime. Identify ways of streamlining (in terms of workload and timelines) high-volume, lower-risk cases.
- Establish and distribute easy-to-use decision support mechanisms for investigators across North America law enforcement agencies to clarify common questions/issues, such as:
  - the equivalent jurisdictions, legal statutes and penalties across regions for categories of economic crime
  - names/numbers of contacts in each jurisdiction
  - how and under which circumstances MLATs should be used
  - minimum levels of evidence required for various actions (e.g., wiretapping, extradition proceedings, etc.)
- Address law enforcement resource shortages in selected cities that are widely-perceived to be low-risk havens for economic crime activities.
- Clarify and communicate widely the responsibilities of various players (e.g., local police detachments are expected to track and report all economic crimes to a central database, even if they lack the ability or resources to investigate at that time).
- Increase the cross-border sharing of information and evidence, within the limits of privacy legislation. (The RCMP is a member of the International Organization on Computer Evidence (IOCE), which seeks to set standards, discuss issues and disseminate information in this area through its network of representatives.)
- Stabilize funding and human resources dedicated to economic crime to ensure an effective response to these increasingly-sophisticated crimes.

TECHNOLOGICAL: ensuring law enforcement and prosecution representatives have access to the tools required for gathering and sharing information effectively

- Increase the level and effectiveness with which information on transborder criminal activities is shared. Measures must be in place to ensure the information is accurate and secure, and that legal parameters of privacy protection are respected in each jurisdiction. (Technology changes are closely tied to legislative changes.)
- Increase usage of existing arrangements such as the US Consumer Sentinel Binational Telemarketing Network (containing data volunteered by victims) to centralize complaint data to spot patterns of fraud. Ensure investigators have reasonable access to computer databases and are trained in sending/retrieving this information.
- Explore the potential (and privacy constraints) associated with sharing Canadian consumer-protection data (e.g., joint Industry Canada / Provincial Government *Canshare* initiative) with US law enforcement counterparts.
- Take advantage of new technologies such as Internet/Intranet networks to share consistent information on policies and best practices to front-line investigators (e.g., step-by-step "MLAT application kit").
- Pursue the possibility of allowing remote testimony (e.g., video links) as evidence in criminal proceedings.

SOCIAL: fostering an environment which discourages the perpetration of economic crimes through high awareness and low tolerance of such acts on the part of the public and the judiciary

- Conserve resources and reduce duplication of effort through the shared development and distribution of educational materials. Undertake and coordinate broad-based information campaigns to educate key segments of the public (e.g., senior citizens) as to the threat and tactics of economic crime.
- Generate a common understanding amongst politicians, judges, prosecutors and investigators as to the seriousness of economic crime, its economic costs to society and the lasting "psychological violence" inflicted on its victims.
- Share results of research studies on economic crime victims and offenders to support the formulation of effective educational materials and crime prevention strategies.

Exhibit IV-7 (cont'd)
Examples of current or proposed Canada/US harmonization initiatives

- Conduct multi-disciplinary reviews of typical end-to-end process steps involved in investigating and processing various categories of economic crime. Identify ways of streamlining (in terms of workload and timelines) high-volume, lower-risk cases.
- Establish and distribute easy-to-use decision support mechanisms for investigators across North America law enforcement agencies to clarify common questions/issues, such as:
  - the equivalent jurisdictions, legal statutes and penalties across regions for categories of economic crime
  - names/numbers of contacts in each jurisdiction
  - how and under which circumstances MLATs should be used
  - minimum levels of evidence required for various actions (e.g., wiretapping, extradition proceedings, etc.)
- Address law enforcement resource shortages in selected cities that are widely-perceived to be low-risk havens for economic crime activities.
- Clarify and communicate widely the responsibilities of various players (e.g., local police detachments are expected to track and report all economic crimes to a central database, even if they lack the ability or resources to investigate at that time).
- Increase the cross-border sharing of information and evidence, within the limits of privacy legislation. (The RCMP is a member of the International Organization on Computer Evidence (IOCE), which seeks to set standards, discuss issues and disseminate information in this area through its network of representatives.)
- Stabilize funding and human resources dedicated to economic crime to ensure an effective response to these increasingly-sophisticated crimes.

TECHNOLOGICAL: ensuring law enforcement and prosecution representatives have access to the tools required for gathering and sharing information effectively

- Increase the level and effectiveness with which information on transborder criminal activities is shared. Measures must be in place to ensure the information is accurate and secure, and that legal parameters of privacy protection are respected in each jurisdiction. (Technology changes are closely tied to legislative changes.)
- Increase usage of existing arrangements such as the US Consumer Sentinel Binational Telemarketing Network (containing data volunteered by victims) to centralize complaint data to spot patterns of fraud. Ensure investigators have reasonable access to computer databases and are trained in sending/retrieving this information.
- Explore the potential (and privacy constraints) associated with sharing Canadian consumer-protection data (e.g., joint Industry Canada / Provincial Government *Canshare* initiative) with US law enforcement counterparts.
- Take advantage of new technologies such as Internet/Intranet networks to share consistent information on policies and best practices to front-line investigators (e.g., step-by-step "MLAT application kit").
- Pursue the possibility of allowing remote testimony (e.g., video links) as evidence in criminal proceedings.

SOCIAL: fostering an environment which discourages the perpetration of economic crimes through high awareness and low tolerance of such acts on the part of the public and the judiciary

- Conserve resources and reduce duplication of effort through the shared development and distribution of educational materials. Undertake and coordinate broad-based information campaigns to educate key segments of the public (e.g., senior citizens) as to the threat and tactics of economic crime.
- Generate a common understanding amongst politicians, judges, prosecutors and investigators as to the seriousness of economic crime, its economic costs to society and the lasting "psychological violence" inflicted on its victims.
- Share results of research studies on economic crime victims and offenders to support the formulation of effective educational materials and crime prevention strategies.

3. Recommended RCMP role in harmonization efforts

The RCMP is being called upon by many stakeholders to increase its level of participation and visibility in harmonization initiatives, and to serve as a focal point nationally for transborder economic-crime law-enforcement discussions. The RCMP, with its national scope and mandate, has the unique ability to serve as a key contact point for Canada/US and multilateral negotiations and discussions in this area. Direct participation of RCMP representatives in talks will be important to ensure that public commitments made are realistic and that sovereign control over economic crime law enforcement on Canadian soil can be properly maintained. Increased RCMP prominence at the international negotiation table will also serve to rebuild the RCMP's credibility and image in the economic crime field.

As the world enters the Internet era, law enforcement must be capable of reacting quicker than ever before, building solid cases based on evidence synthesized from multiple sources inside Canada and abroad. Canada's current laws and policies were, for the most part, conceived and adopted at a time before "high tech" crimes (with thousands of geographically-scattered victims) became prevalent. Given this dramatic change in context, the RCMP must work proactively with the respective Justice Departments as well as with other partner agencies across Canada and the US to adapt to and to shape a modernized law enforcement environment and to develop a "North-American response" to key economic crime problems.

V

Stakeholder Feedback

Over the course of this study, KPMG interviewed and/or conducted focus groups with a variety of stakeholders of the Economic/Commercial Crime Program. Approximately 80+ individual interviews were conducted with representatives of federal and provincial governments, financial institutions, private sector corporations, etc. As well, approximately 50+ representatives from stakeholder organizations participated in a number of focus groups held across the country.

In this chapter we provide a summary of the main issues that were raised during these individual and group meetings. In conducting these meetings, KPMG consultants found a great deal of consistency in viewpoints across the country between both private and public sector participants, along with an extremely high degree of frustration with the current level of service being provided. As agreed with stakeholders to ensure anonymity and confidentiality, an aggregation of their views is provided below. A complete list of stakeholders contacted is provided as Appendix A to this report.

We have organized the feedback received under the following headings:

- Trends.
- Process issues.
- Communication and cooperation.
- Resource allocation.
- Human Resources.
- Technology.

A. Trends

Stakeholders identified the following trends which they believe to be critical in addressing economic crime both now and in the future.

1. Organized crime is becoming a greater threat in the commission of economic crime in Canada

The economic crime threat in Canada is no longer localized to one or two specific cities or areas of the country, but is becoming more national and even international in scope. Organized crime groups may be headquartered in Canada. Increasingly, however, the organized crime threat is comprised of different ethnic groups located in other countries and perpetrating crimes in Canada. These groups are becoming more technologically sophisticated and are expanding into all areas of economic crime through the use of the Internet. Organized crime groups are targetting vulnerable groups such as seniors (e.g., telemarketing) and their activities are resulting in considerable losses and possible ruination of individuals or groups of individuals (e.g., group RRSP holders, etc.). Moreover, these groups are hard to track and to investigate. Crimes are often multi-jurisdictional in nature, potentially falling under the purview of municipal, provincial police forces or the RCMP. As well, there is often an international component which requires dealing with foreign governments, international agencies and foreign policing institutions. These multi-jurisdictional issues add significantly to the complexity of these crimes and the subsequent complexity and cost of the investigative process.

2. Canada is increasingly being perceived as a safe haven for perpetrators of economic/commercial crimes

Due in large part to inadequate resourcing, many economic/commercial crimes are not investigated and/or not prosecuted, thereby allowing criminals to go unpunished. As well, with the onset of "conditional sentencing", the power of the legal system has become inadequate. Even in those cases where perpetrators are found guilty, often the punishment is minor or commuted from a prison sentence to a fine and/or community service. This situation has tarnished Canada's image on the international stage and resulted in Canada becoming a very attractive spot for economic crime.

3. Stakeholders are seeing an era of tremendous growth in economic crime

Stakeholders are seeing growth in economic crime including such areas as: large company fraud; bankruptcies; telemarketing fraud; counterfeit cards; securities fraud; charitable organization fraud; etc. They see this era as a breeding ground for "white collar" crime. Stakeholders view the legal system as having "no teeth" and the Charter of Rights and Freedoms as reducing the RCMP's ability to move quickly in obtaining search warrants and following up on suspicious events. As well, with the aging of the "baby boomer" population and the increased risk-taking in investment of both disposable income and retirement savings, the general population is becoming more and more vulnerable to attack.

4. The trend in government downsizing at all levels over the past ten years is resulting in greater risk to our public institutions and infrastructure

Stakeholders believe that the decimation of the middle management ranks of government has resulted in much less overall monitoring of government programs. Reduced budgets de-emphasize instituting appropriate controls and security measures for public programs. This situation has allowed programs to become increasingly vulnerable to the criminal element and will continue to open up greater and greater opportunities for program abuse, fraud, technological crime, etc.

B. Process

From a process perspective, stakeholders across the country raised a number of issues which they believe need to be addressed.

1. Stakeholders see no national vision or direction for Economic Crime

As indicated previously, stakeholders anticipate a significant increase in economic crime in the future. They are very concerned about this situation as they see no national vision/strategic direction in place within the Force to deal with this issue. Stakeholders perceive a lack of national direction and no national service delivery framework to ensure coordination or consistency in the provision of service. As well, they see no evidence of any trend analysis being done regarding the current state of economic crime as well as areas of future growth.

2. Stakeholders view the end-to-end process as dysfunctional

Not only do stakeholders perceive inadequate analysis in the Force of economic crime trends and issues and their consequent impacts on Canada, they have little faith in the total process from the determination of criminal activity, the conduct of investigations, and throughout the judicial process. Stakeholders indicated that they were unaware of any criteria used by the Economic Crime program or Commercial Crime sections across the country to select and/or priorize cases for investigation. Stakeholders do not know if the Force will or will not investigate the cases they present. If cases are accepted for investigation, these cases are often inadequately/inappropriately resourced. This results in lengthy investigations subject to the risk of evidence and/or witness disappearance or death, etc. Cases lose strength over a lengthy investigative timeframe and are not regarded favourably by the prosecutorial and judicial system. As well, there are lengthy delays and insufficient penalties in the judicial system which have little or no deterrent effect.

Stakeholders expressed considerable frustration that no control or coordination exists within the overall process.

3. Stakeholders view the response rate for cases accepted by Economic Crime/Commercial Crime sections to be neither timely nor efficient

Stakeholders indicated that they can submit cases to Commercial Crime sections and wait weeks or months just to obtain a decision as to whether or not the case(s) will be investigated. This situation results in a high degree of frustration among stakeholders and they often give up. Where possible, stakeholders then pursue a potentially less optimal civil or administrative avenue in order to achieve some means of retribution for offences.

4. Stakeholders view Economic/Commercial Crime management practices to be fragmented

Stakeholders believe that the lack of leadership and management focus has eroded Economic/Commercial Crime over time. This situation has resulted in a deterioration in skill levels of investigative officers and the consummate deterioration in quality of services provided. Stakeholders perceive a lack of commitment to the importance of the economic crime program evidenced in the lack of continuity amongst units across the country, an ongoing lack of resources/removal of resources, and a fragmentation in levels of authority and accountability across program management levels. They are frustrated and annoyed that their cases are not being addressed and that the local/division operational managers evidence a lack of interest in pursuing their investigations.

C. Communication and cooperation

Stakeholders across the country highlighted some serious concerns regarding the sharing of information and the need for enhanced partnering with Economic Crime.

1. Insufficient information is shared between stakeholders and Economic/Commercial Crime

Stakeholders for the most part felt "out of the loop" when it came to Commercial Crime sections sharing information regarding the screening process for cases, how priorities were set and which cases were being accepted or rejected. No consistent practices/process for ongoing communications with stakeholders exist across the regions. Some stakeholders indicated that communications with individual units was working well, but these models depended heavily on a commitment to strong client relations, regular meetings, and the skills and interest of both the investigators and managers involved.

In the Greater Toronto Area (GTA), stakeholders complained repeatedly about the communications problems resulting from the re-location of detachments from Toronto to the outlying areas. Some stakeholders were so frustrated that they had decided not to share useful national and international contact names because by the time these stakeholders were able to get in touch with appropriate investigators, other priorities took precedence.

2. Stakeholders are anxious for greater consultation/partnering early in the process

The majority of stakeholders consulted are well aware of the resource restraints facing Economic/Commercial Crime. As well, they are aware of the increasing multi-jurisdictional and complex nature of cases. Stakeholders realize that the Force cannot "do it all" and they indicated a willingness to work more closely with the Economic Crime program. They are interested in understanding the process better, to share pertinent information, to clarify and communicate needs and to work with the Economic Crime program to expedite investigations. Many of the these organizations have complementary skills which could be utilized effectively without comprising the objectivity of RCMP investigators.

D. Resource allocation

Stakeholders across the country recognized resource allocation as a major issue for the Economic Crime program.

1. Stakeholders agree that the Economic/Commercial Crime program is under-resourced

Many stakeholder organizations are conducting their own analysis of current and potential future levels of economic crime activity. They indicate that crime statistics do not reflect accurately the actual level of economic crime. To address this reality, these organizations are establishing investigative services or increasing resources to their existing programs to combat this situation. These resources are dedicated to doing investigations focused on lack of compliance with regulatory requirements within the purview of a particular organization and/or the conduct of preliminary "leg work" to collect data, interview witnesses, prepare documentation prior to submission to the RCMP for investigation. Many highlight that due to the lack of appropriate resource levels within the Economic/Commercial Crime program, they have had to enhance their own programs, otherwise they would have little or no chance of having the Force even consider their cases. Stakeholders observe that the Economic/Commercial Crime is currently resourced to address crime levels that existed approximately ten years ago, whereas the level of economic crime activity has increased significantly since that time.

2. Cases submitted to the Economic/Commercial Crime program may or may not be accepted

Stakeholders highlight that even when much of the preparatory work has already been done on cases prior to submission for investigation, they are still not confident that their cases will be taken. If accepted for review, cases often sit on investigators' desks for weeks or months pending a review to determine whether or not they will be investigated. Commercial Crime sections indicate that there are just not enough investigators to even review the information to make a decision. Stakeholders are extremely frustrated with this situation and find this lack of service completely unacceptable.

3. An insufficient number of Commercial Crime prosecutors currently exists to handle the potential number of cases arising

Stakeholders indicated that not only were their insufficient resources Economic/Commercial Crime to address all their cases, but a similar situation exists at the prosecutorial level as well. This was particularly critical in the event that stakeholders are seeing an overall increase in economic crime activity and are only seeing a small percentage of cases being pursued actively. They believe that any increases considered for the Economic/Commercial Crime program within the RCMP should be mirrored in the judicial system so ongoing delays are not perpetuated.

E. Human Resources

In the Human Resources area, stakeholder concerns dealt with skill levels required to handle both larger and smaller cases. Overall, stakeholders felt that the skill levels within Economic/Commercial Crime were deteriorating and need to be augmented.

1. Pursue smaller, as well as larger, cases to provide a good investigative training ground

Many stakeholders felt that local Commercial Crime sections were rejecting smaller, less complex cases in favour of the larger, higher profile investigations. Concern was expressed over this trend as stakeholders believed that some of the smaller cases being rejected had greater potential for obtaining a conviction and could also act as a deterrent to future criminal activity. As well, though these cases often involved smaller dollar figures, they often had more serious impacts on individual victims. As well, stakeholders indicated that these cases potentially could provide an effective on-the-job learning environment to enhance skill levels of investigators new to the program.

2. Economic/Commercial Crime cannot off-load larger, complex cases to local police authorities

Concern was expressed that although skill levels in Economic/Commercial Crime had been deteriorating over time, these skill levels were still higher and more comprehensive than those in Commercial Crime units in local police forces. To that end, divesting larger, more complex cases to local Forces would further deteriorate the quality of services. Instead stakeholders felt that Economic/Commercial Crime should cooperate more closely with these local Forces and provide strong leadership in the effective conduct of investigations.

F. Technology

All stakeholders acknowledged the increase in use of technology by organized crime groups and the need for the RCMP to address this issue.

1. RCMP needs to take a leadership role in technology

Stakeholders acknowledged that, increasingly, economic crimes were being perpetrated through the use of technology and involved significant national and international implications. Therefore, as part of the national police force, Economic/Commercial Crime should provide assistance and leadership in the area of technology to its stakeholders and other police forces.

VI

Commercial Crime Member Feedback

Over the course of this study, KPMG interviewed a number of Economic/Commercial Crime managers as well as representatives of other RCMP programs. In addition, as KPMG travelled across the country, we held sessions with all Commercial Crime members who indicated an interest. The purpose of these sessions was to provide a status report on the project and to allow members to express their ideas. The sessions were very well attended and members were very vocal about their concerns. Many concerns mirrored and supported issues that were raised by stakeholders in both their individual interviews and focus group sessions. Below we provide a summary of issues raised by members.

We have organized the feedback received under the following headings:

- Process issues.
- Communication and cooperation.
- Resource allocation.
- Human Resources.
- Technology.

A. Process issues

1. No national strategy, national standards exist currently

In line with stakeholder views, members are concerned that no national direction or strategy nor national standards currently exist for Economic/Commercial Crime. They believe that both current and future trends and issues, their implications for Economic Crime and the impacts on the public and stakeholder groups are not being identified and analyzed. Members believe that each area of the country is "doing its own thing" resulting in an inconsistent and uncoordinated approach to service delivery. They see little or no sharing of information or best practices across the country and feel isolated in only being able to draw upon their immediate area for support.

2. Members echo stakeholder concerns regarding ineffective management practices in Economic/Commercial Crime

Reiterating stakeholder views, Commercial Crime members are very concerned about the lack of vision, strategic direction, and leadership in Economic/Commercial Crime. They see positions remaining vacant over long periods of time while investigators are spending excessive hours on cases and other viable cases are being rejected due to lack of manpower. Members see their colleagues being assigned to other duties and consequently leaving their ongoing cases on hold/uncompleted.

Members also indicate that the current program has little or no control over its own destiny as well as its ongoing day-to-day operations. Managers may or may not have the appropriate level of authority to make budgetary/resourcing decisions. Delegation of authority is highly dependent on the management structure of the division/region. Overall, members see little or no evidence of support of the Economic Crime program by RCMP senior management and believe, like stakeholders, that left this way, the program will die a slow death.

3. Program support services have dwindled over time

Coupled with ongoing reductions and ineffective management practices, members indicate that investigators spend a significant portion of their time on administrative and clerical duties as well as investigative support duties (e.g., file opening and maintenance of ongoing documentation, classification and cataloguing of evidence, background research, etc.) when they should be focusing their effort on more in-depth and technical investigative duties.

As well, those investigators involved in Tech Crime cases or who have demonstrated any type of technological interest or know-how indicate that they are spending considerable time providing in-house technical support to the Commercial Crime sections as well as other programs because in-house Informatics Support is unavailable.

4. Commercial Crime activities are in reactive mode

Both stakeholders and members alike see the Economic/Commercial Crime program stuck in a reactive "crisis management" mode. Members believe that due to the current state of the program, they are only able to react to cases/complaints that "come in the door". They believe, as do stakeholders, that the program should be placing more emphasis on prevention and education of both the public in general as well as stakeholder and client groups. Members strongly believe that both managers and investigators alike must be more involved in enhancing public awareness of economic crime threats, must participate in industry associations to learn from experts in the field and form effective working relationships, and work more closely with other enforcement agencies to develop proactive crime prevention programs. Members and stakeholders alike believe that currently the Economic/Commercial program has no public image. A higher, more proactive profile for Economic/Commercial Crime across the country would contribute significantly to both crime deterrence and prevention.

5. Members spend too much time on activities outside the mandate

Members indicated that they are spending considerable time on investigations/special assignments outside of Commercial Crime. Although both members and stakeholders believe that the program's skill and experience levels have deteriorated over the past number of years, investigative and technical skills in Commercial Crime are still often more sophisticated than in other programs. Therefore, investigators are often requested/assigned to assist other programs (e.g., pornography on the Internet, etc.) or are assigned to special events or major incidents occurring in their areas. While everyone is in agreement that as part of the duties of a national police force, the Economic/Commercial Crime program must also participate in these types of activities, no provision is made for continuation of ongoing cases and/or communication of these special requirements to clients. This situation results in a high degree of frustration on the part of both members and stakeholders alike.

6. An enhanced team approach is required

Members supported stakeholders strongly in their belief that more of a "teaming" model should be employed across the country. They felt that in many cases investigation timeframes could be significantly reduced and results provided in a more timely fashion if investigators worked within a team approach combining both specialized and multi-disciplinary skills, as appropriate. In addition, members indicated that working within such a model would allow for greater mentoring of new/junior investigators and provide enhanced skills development opportunities while fostering increased continuity on cases.

7. Focus on end-to-end process

Both members and stakeholders alike agreed that not all problems in Economic/Commercial Crime rested with the Force. They recognize that delays are also occurring in the judicial system with insufficient numbers of prosecutors, delays in court time, and insufficient penalties attributed to convictions. Improvements are required throughout the end-to-end process.

B. Communication and cooperation

Both stakeholders and members alike highlighted the need for greater communication and cooperation between all parties involved in the Economic/Commercial Crime.

1. Need for increased partnering

Members agreed very strongly with stakeholders that Economic/Crime needs to work more closely with clients and stakeholders to exchange critical information, share best practices, identify priorities, discuss ongoing cases and clarify criteria for accepting/rejecting cases. Members see this as having significant potential in exchanging important information, making informed decisions, and capitalizing on knowledge and resource availability in stakeholder organizations. As well, members acknowledge that they have to work much more closely with other enforcement agencies/authorities on a local, national and particularly international basis to address multi-jurisdictional and complex cases, arising more and more frequently. Where cooperative/partnering models are currently in place across the country, both members and stakeholders find them to be very effective.

This increased partnering/teaming model will be even more critical in the future in order to share expertise and capitalize on the ability of investigative teams to use resources external to the Force to formulate multi-disciplinary teams.

2. Members are skeptical change will happen

Although members are very much in support of the changes required to improve the effectiveness of Economic/Commercial Crime, they are very skeptical that any change will happen. They indicated that for major change and improvement to occur, not just the support of Commercial Crime/Economic Crime managers is required. Members believe strongly that Senior RCMP Management must actively support any changes and provide ongoing commitment to program success. As well, Senior Management must attract and retain the attention of political authorities in order to ensure that appropriate levels of resources are provided to support national and international commitments made in the political forum.

C. Resource allocation

Ongoing cutbacks and lack of appropriate resource levels is a major concern for members.

1. Need for resources throughout end-to-end process

Members, in line with stakeholders, indicated that appropriate resourcing levels were not only required within the Economic/Commercial Crime program but at the prosecutorial level as well. They evidenced concern that too many legitimate cases were being rejected due to lack of resources to investigate as well as to prosecute. Members felt that increasing resources for investigations would only address part of the problem and that consideration would need to be given to having commensurate increases at all levels. Otherwise, if more cases were investigated and submitted for prosecution, these cases would either be rejected or become severely delayed at the judicial level. This situation would then send even poorer messaging to the criminal element than that which was currently taking place.

D. Human resources

Human resources management issues are of great concern to members.

1. Members are distraught

Morale amongst members across the country is very low. Many members are emotionally distraught not only over ongoing cutbacks but also over the overall state of the Economic/Commercial Crime program. These members are very dedicated. They feel they have invested their time and commitment to the program and have seen little return on that investment from the program as a whole and RCMP management as a whole.

2. Systemic human resources management issues are critical

Members, like stakeholders, are very concerned about the systemic human resources management problems which currently exist and have existed over time within the Force. They are frustrated with the skill level of investigators, the lack of resources and commitment to ongoing learning and development, and the inability of the program to attract and retain qualified staff. Members are aware of the lack of promotional opportunities or career path within the program and, like stakeholders, see an ongoing exodus of capable individuals to other programs for promotional opportunities or to external organizations to obtain more appropriate recognition and reward. Members are aware that the Economic/Commercial Crime has little or no say in the staffing of positions and few ways of addressing poor/inadequate performance. An ineffective structure, coupled with a lack of control over human resources management practices, frustrates and alienates members at all levels.

3. The para-military structure is not appropriate for Economic Crime

Both stakeholders and members believe that the para-military rank structure is no longer appropriate for Economic Crime. More and more as the Economic Crime field evolves and becomes more sophisticated, so must investigators, who need more specialized knowledge and skills to obtain and maintain credibility in the field. Members believe that Economic Crime is truly becoming a "specialist" program requiring a more flexible classification and remuneration system.

E. Technology

1. The need for appropriate technology support is paramount

Members indicate that it is becoming increasingly more difficult to perform their duties with the level of technology tools and support that currently exists across the country. Investigators do not have appropriate hardware and software, along with commensurate training in its use, to be able to compete with the criminal element, particularly organized crime. Organized crime groups are sophisticated. These groups make extensive use of technology involving themselves in multi-jurisdictional criminal activities and investigators are unable to keep pace. Members believe that the lack of appropriate technology and the skills to use it severely hampers their ability to conduct timely and effective investigations.

VII

Recommended Organization Structure For Economic Crime

In this chapter we describe the recommended high-level conceptual organizational configuration for Economic Crime. For this organization structure, we have assumed that Economic Crime will encompass both the services provided by the Economic Crime Branch at NHQ as well as the services provided by Commercial Crime Branches and Sections currently reporting within the regions across the country.

A. Key factors driving changes to Economic Crime

In our discussions with Stakeholders and Economic/Commercial Crime members across the country, a number of issues which stress the need for change, were brought to our attention. The following issues or "drivers of change" were considered carefully in our deliberations concerning the recommended organizational configuration:

- Organized crime is becoming a greater threat in economic crime in Canada. As well, this threat is becoming more national and international in scope.
- Canada is increasingly being perceived as a safe haven for perpetrators of economic crimes. Due to inadequate resourcing and the increasing multi-jurisdictional nature of economic crimes, confusion exists as to which policing agency will assume responsibility for investigations. This shuffling of cases between authorities, along with an inadequate level of resourcing often results in cases "falling through the cracks".
- Stakeholders are seeing an era of tremendous growth in economic crime with the onset of the aging of the "baby boomer" population, the greater risks being taken in investment of disposable income and retirement savings, as well as the increase use of technology for all types of economic transactions.
- Little or no leadership and vision in Economic Crime over time has resulted in a lack of strategic direction or national strategy in place for Economic/ Commercial Crime.

- No national service standards, nor coordination or consistency in service delivery are currently in place to deal with growing nationalization and internationalization of economic crime activities and the increasing involvement of organized crime groups.

- A lack of Senior Management commitment to the importance of Economic/Commercial Crime has resulted in an erosion of the program over time. Management practices are fragmented, no continuity in Commercial Crime units exists across regions, skill levels are deteriorating, inadequate resourcing exists and there is an ongoing high vacancy rate in federal positions.

- Response rate to cases submitted by Stakeholders is neither timely nor efficient. No consistent criteria exist to select/reject and/or priorize cases.

- Little information is exchanged/shared with stakeholders due to lack of standard practices in place. Good communications with clients exist only where local management has incorporated a customer focus. Little or no sharing of best practices/lessons learned exists across the country.

- The use of technology is growing. Not only can technology be the victim of crime but organized crime groups as well as individual fraudsters are becoming increasingly more sophisticated in their use of technology as a medium for crime on a national and international basis.

- The current focus of activities is reactive. Little is currently being done in the area of public/client education and awareness, public image and profile building and overall crime prevention.

B. Current organizational model

The current organizational model splits responsibility for economic crime between the Economic Crime Branch at Headquarters and the Commercial Crime Branches and Sections reporting through the regional structure.

1. Headquarters

Economic Crime policy and program development responsibilities reside in the Economic Crime Branch. The Branch develops policy and program directives for Economic Crime including Technological Crime, Market/Securities Fraud, Commercial Fraud, Counterfeiting and Federal Statutes. The Branch does some trend analysis and maintains relationships with external agencies, other policing authorities, and international organizations. However, the Branch has no direct authority or accountability for Commercial Crime units and/or investigators in the field.

2. The field

In the field a variety of approaches exist. Some divisions have Commercial Crime Branches at divisional headquarters and some do not. Some divisions are divided into sub-divisions with Commercial Crime sections operating within each sub-division. Other divisions have Commercial Crime sections at the detachment level.

In "contract policing" provinces, Commercial Crime sections include both federal and provincial Commercial Crime positions. As well, these sections may encompass Customs and Excise and GIS functions in some of the smaller regions/divisions.

The result is a fragmented, reactive and uncoordinated and/or inconsistent service delivery model. Commercial Crime sections are subject to the priorities of the division/region, which while very valid in their own right, often result in long-term vacancy rates in federal positions. These surplus salary dollars are then used to satisfy operational requirements (e.g., new police cars, radar guns, gas, etc.). Due to budgetary constraints, little in the way of skills development and continuous learning takes place. Regional/divisional priorities of necessity take precedence over any type of focus on Economic/Commercial Crime.

C. Recommended conceptual organization model for Economic Crime

1. Introduction

According to accepted organizational development theory, organizations as organisms evolve over time. As such, they go through different stages of development throughout the maturation process, as their environments and client needs change. It is critical, therefore, that organizations realize that they have to evolve to stay current, respond to client needs, and continue to survive.

Although organizational theorists classify the phases of development somewhat differently, essentially there are four stages of an organization's evolution.

Phase 1

As organizations start out, they are often unsure of how to manage and control their business. As such, they begin in a very control-oriented manner. This often works well when the organization is small and less diversified.

However, as the organization grows, becomes much more diverse in its business activities, and responds to a wider client/population base, it must rethink its management and control structure.

Phase 2

As this growth and diversification continues, the field requests strongly that the centre "loosen the reins". Having all decisions funneled through Headquarters is time-consuming and the field always feels that Headquarters doesn't communicate well enough to really understand the needs of front-line service delivery. Therefore, significant pressure is applied to the centre to decentralize some decision-making. In response to this pressure, the centre does just that. Everyone finds that this seems to work well.

Phase 3

Since some decentralization of authority seems to work well, the next question becomes—why not decentralize everything? More and more responsibility and authority, therefore, is delegated to the field and only staff and policy functions tend to remain in Headquarters. However, as is often the case, although the authority is decentralized, no accountability framework is established so that the centre is able to monitor business activities and/or service levels across the organization effectively. Where the same business activities need to be done and consistent service levels are required in order to meet requirements of national or multi-national clients, lack of any authority at the centre results in every decentralized component "doing its own thing". This becomes a higher risk to the organization, particularly if the services provided require specialized skills and an ongoing commitment to skills and knowledge upgrades, to ensure effective service provision and client satisfaction on a national basis.

Phase 4

Ongoing growth and evolution of the organization then suggest the need for some direction and leadership from the centre to ensure overall consistency and coordination in service delivery. For organizations that have a national mandate, this means the need for a national focus and the institution of a more centralized reporting framework.

This centralized structure, however, is not the command and control configuration which characterizes Phase 1. It is, of necessity, a much more flexible and empowered structure. The centre provides a national focus, acts as a conduit for the storage and exchange of critical information across the country, and provides strong and committed value-added leadership to line operations in the field. Field managers are an integral part of the overall management team and have delegated levels of responsibility and authority appropriate to accomplishing their business objectives. They are held accountable through mechanisms such as performance contracts and established performance measures for the effective achievement of those objectives.

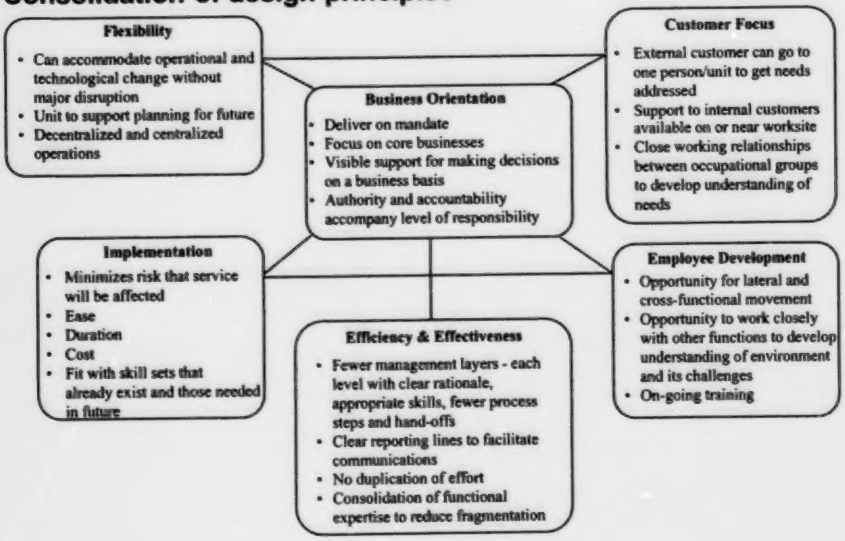
An organization is only ready to move to this phase of evolution if there is up front commitment at Headquarters and from the field to work together closely to manage a quality organization committed to client service.

What we have recommended for Economic Crime is just such a Phase 4 organizational model. In developing the recommended organizational structure, we were guided by a set of organization design principles agreed during workshops and interviews across the country. These principles helped focus the design of the structure on its business orientation, the flexibility to manage change, the internal and external customer service focus, the ongoing need for employee learning and development, the optimization of efficient and effective service delivery, and the flexibility to implement the model.

Exhibit VII-1 highlights the design principles. An analysis of the recommended model against these principles is presented as Section D following a more detailed discussion of the recommended model.

As well, a more detailed list of the design principles is provided in Appendix C to this report.

Exhibit VII-1
Consolidation of design principles



Flexibility

- Can accommodate operational and technological change without major disruption
- Unit to support planning for future
- Decentralized and centralized operations

Customer Focus

- External customer can go to one person/unit to get needs addressed
- Support to internal customers available on or near worksite
- Close working relationships between occupational groups to develop understanding of needs

Business Orientation

- Deliver on mandate
- Focus on core businesses
- Visible support for making decisions on a business basis
- Authority and accountability accompany level of responsibility

Implementation

- Minimizes risk that service will be affected
- Ease
- Duration
- Cost
- Fit with skill sets that already exist and those needed in future

Employee Development

- Opportunity for lateral and cross-functional movement
- Opportunity to work closely with other functions to develop understanding of environment and its challenges
- On-going training

Efficiency & Effectiveness

- Fewer management layers - each level with clear rationale, appropriate skills, fewer process steps and hand-offs
- Clear reporting lines to facilitate communications
- No duplication of effort
- Consolidation of functional expertise to reduce fragmentation

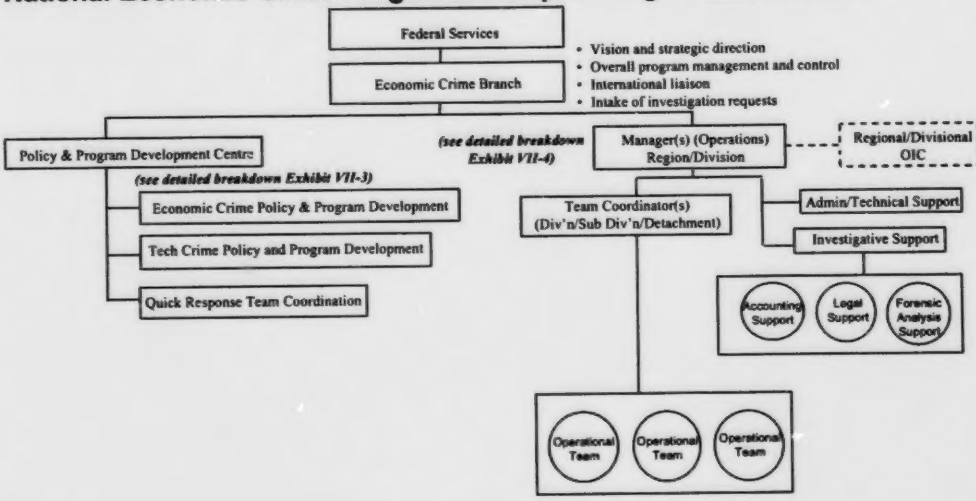
2. Recommended model—A National Economic Crime Program

A number of organizational models were discussed in workshops/focus groups held across the country. These options went from maintenance of the status quo right through to the establishment of a separate agency for Economic Crime. Each option was discussed and analyzed by KPMG in conjunction with input from RCMP staff and stakeholder representatives. The models which were not chosen are provided in Appendix D to this report.

Although each option had a number of advantages and disadvantages, the option which addressed the most critical current and future needs of Economic Crime, was a National Economic Crime Program/Service Line reporting to the Director of Federal Services.

The recommended model is described in detail below, following which is an assessment of the model against the organization design principles, and a discussion of the reasons why this model was chosen, as well as some considerations for implementation.

Exhibit VII-2
National Economic Crime Program conceptual organization model



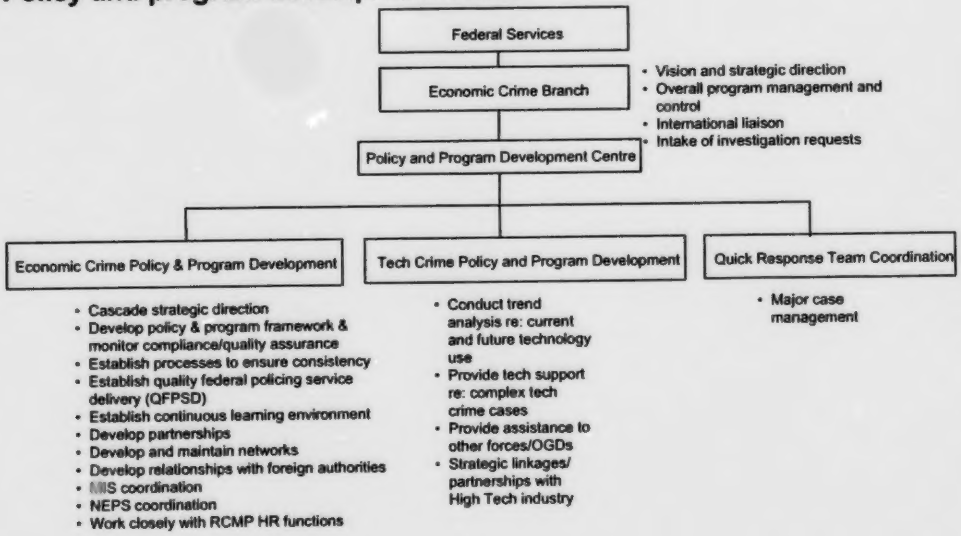
Federal Services
Economic Crime Branch
• Vision and strategic direction
• Overall program management and control
• International liaison
• Intake of investigation requests
Policy & Program Development Centre
(see detailed breakdown Exhibit VII-3)
Economic Crime Policy & Program Development
Tech Crime Policy and Program Development
Quick Response Team Coordination
(see detailed breakdown Exhibit VII-4)
Manager(s) (Operations) Region/Division
Regional/Divisional OIC
Team Coordinator(s) (Div'n/Sub Div'n/Detachment)
Admin/Technical Support
Investigative Support
Accounting Support
Legal Support
Forensic Analysis Support
Operational Team
Operational Team
Operational Team

a) National Economic Crime Program Head

In this model, the Head of the National Economic Crime Program would report directly to the Director of Federal Services. The Head of the Program would be ultimately responsible for setting the vision, strategic direction, and overall national strategy for the National Economic Crime Program/Service Line. The Program Head would assume responsibility for overall program management and control with full responsibility and accountability for all program financial and human resources. Accountability for the day-to-day management of these resources would be delegated appropriately to operational managers across the country. As a national program/service line, all human resources would report centrally through local Managers of Operations to the Head of the National Economic Crime program.

A more detailed description of responsibilities of the Policy and Program Development and Field Operations components of the program is provided in Exhibits VII-3 and Exhibit VII-4 following.

Exhibit VII-3
Policy and program development centre


Federal Services
Economic Crime Branch
Policy and Program Development Centre
Economic Crime Policy & Program Development
Tech Crime Policy and Program Development
Quick Response Team Coordination

- Vision and strategic direction
- Overall program management and control
- International liaison
- Intake of investigation requests

- Cascade strategic direction
- Develop policy & program framework & monitor compliance/quality assurance
- Establish processes to ensure consistency
- Establish quality federal policing service delivery (QFPSD)
- Establish continuous learning environment
- Develop partnerships
- Develop and maintain networks
- Develop relationships with foreign authorities
- MIS coordination
- NEPS coordination
- Work closely with RCMP HR functions

- Conduct trend analysis re: current and future technology use
- Provide tech support re: complex tech crime cases
- Provide assistance to other forces/OGDs
- Strategic linkages/ partnerships with High Tech industry

- Major case management

b) Policy and Program Development Centre

The Policy and Program Development Centre would potentially be divided into three key units: Economic Crime Policy and Program Development; Technological Crime Policy and Program Development; and the Quick Response Team Coordination function.

The Centre's mandate would be two-fold. It would encompass policy and program direction to the field as well as provide analytical support to Senior Management decision-making with the Program, Federal Services and the

Force as a whole regarding the current and future state of Economic and Tech Crime and the implications for Canada.

As well, a significant focus of the Centre would be a proactive one to develop and enhance awareness of Economic Crime on a national basis with both the public and stakeholder groups. The Centre would develop the image of the Economic Crime Program focused on consistent and coordinated proactive public education and prevention messaging. This would be enhanced through establishing an Economic Crime presence on taskforces/committees with other governments, law enforcement authorities, industry associations, and at critical fora on a national and international basis.

i) Economic Crime Policy and Program Development unit

The Economic Crime Policy and Program Development unit would exist at National Headquarters and be enhanced to add greater value to field operations. It would be comprised of a strategic, multi-disciplinary proactive team. This unit would be responsible for working in conjunction with the field and as well as other policy and program development functions across Federal Services to establish flexible and enabling policies and practices and coordinate the operationalization of Program strategic direction.

The unit would develop and monitor Economic Crime policy and standards of practice, establish guidelines for processes and procedures such as complexity rating and/or case screening guidelines, etc. to ensure consistency across the country. As well, the unit would establish partnerships and strategic alliances with other policing authorities and stakeholder groups at the national level. The unit would facilitate relationships/partnerships with foreign governments and foreign authorities to ensure more rapid access to information and quick turnaround on cases with international connections and implications.

The unit would also foster sharing of information and best practices across the national program and ensure the appropriate functioning of the MIS and NEPS systems in support of program operations. Along with the Tech Crime Policy and Program Development Unit, this unit would work closely with the RCMP Learning and Development Division to establish and maintain a continuous learning environment across the program.

In support of efficient and effective Senior Management decision-making regarding the current and future state of the Economic Crime, the unit would require a capability to conduct research and statistical analysis of current and future trends in Economic Crime. Through analysis of historical and current Economic Crime data as well as the analysis of future trends in the economy and areas of economic growth on both a national and global basis, the unit could investigate and forecast future crime trends/growth. This data would provide critical support to the Program Head and Senior Management regarding the need to refocus efforts, change processes, shift resources, etc.

ii) Tech Crime Policy and Program Development unit

For purposes of discussion here, we have defined Tech Crime as encompassing crimes not only where the computer and/or telecommunications system are the targets of the crime but crimes where technology is being used as the medium of commission.

Tech Crime is a growing area as the Canadian population relies more and more heavily on technology to conduct its economic business. To address this growth, we recommend setting up Tech Crime as a separate unit within the Policy and Program Development Centre. This unit would support Tech Crime services across the country. Its focus would be national in scope and direction.

The Tech Crime Policy and Program Development function would exist at national headquarters. This multi-disciplinary team would be a proactive and strategic group responsible for working in conjunction with other functions, such as High Tech Crime Forensics (HTCF) in Technical Operations Directorate, to establish and incorporate the strategic direction of Tech Crime within the overall operational framework of the Force. The unit would develop and monitor Tech Crime policy and standards of practice, establish processes and procedures to ensure consistency in application across the country and minimize risk of loss of key electronic evidence in the conduct of investigations. The unit would also work closely with the RCMP Finance and Informatics Directorates to establish resource and technology support requirements for Tech Crime, and also with Tech Crime Investigators and Computer Investigative Support personnel in the field to provide required information and support for operations. This infrastructure would include establishing the necessary processes across the country; standards of practice; standardized coding practices for case types and levels of complexity. The unit would also track technology assistance provided to other crime areas; and would measure results achieved by Tech Crime practitioners.

As well, the unit would be responsible for the ongoing development of the Tech Crime program through the establishment of partnerships and strategic alliances with the High Tech industry. It would foster sharing of information and best practices regarding Tech Crime investigations across the country and on an international basis. Along with the Economic Crime Policy and Program Development unit, it would also work closely with the RCMP Learning and Development Division to establish a continuous learning environment to improve basic technology knowledge and skills in Economic Crime investigators and facilitate the ongoing skills upgrades required by these investigators.

The Tech Crime Policy and Program Development unit along with the field staff would develop a pool of external experts across the country with specific areas of expertise (e.g., encryption methods, operating systems, etc.) which could be accessed quickly by all regions/divisions to address investigative needs.

In support of efficient and effective Senior Management decision-making regarding current and future RCMP Tech Crime services, the Tech Crime Policy and Program unit would also require a capability to conduct research and statistical analysis of current and future trends in Tech Crime. Analysis of both historical and current Tech Crime data, and investigation and forecasting of anticipated future trends/growth areas on a national and global basis would be conducted. Along with general Economic Crime information, this data would provide a critical information base for Senior Management to facilitate decisions regarding the need to refocus efforts, change processes, shift resources, etc.

A significant focus of the Head of this unit would be to develop and enhance awareness/education of groups/organizations on a national and regional basis as to trends in Tech Crime and methods to employ to enhance security of information/telecommunications systems. Partnering through the establishment of task forces/committees with Industry groups on a national and international basis would provide the best opportunity to develop greater awareness, and to educate and ensure consistent messaging regarding Tech Crime, now as well as in the future.

iii) Quick Response Coordination

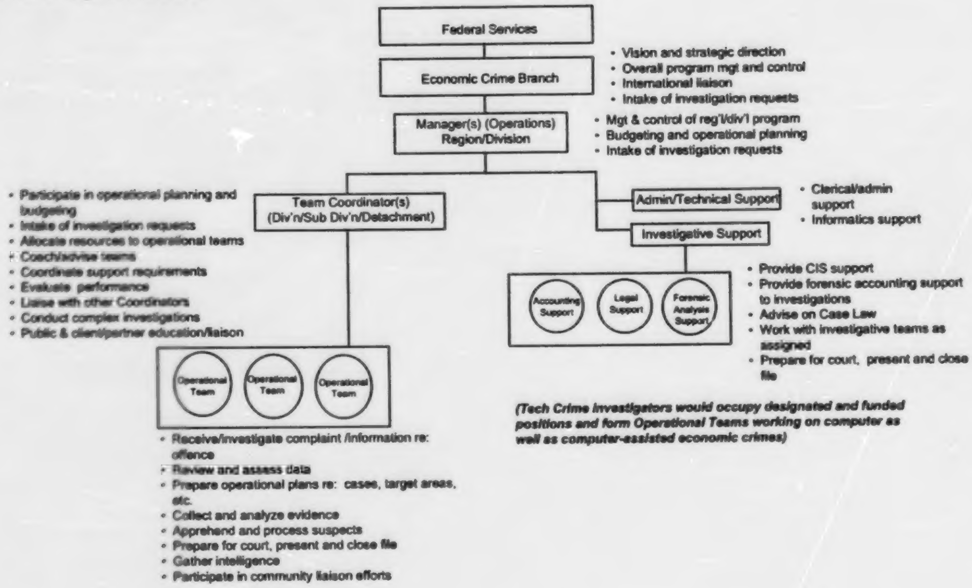
A Quick Response Coordination function has been recommended to address the need to set up national teams to handle major cases (e.g., Bre-X, Airbus, etc.) which arise on an ongoing basis. At present, there is no national mechanism to staff and resource these types of cases quickly and effectively.

This Quick Response Coordinator would provide just such a national mechanism. The position would use a major case management model with the ability to draw on appropriate resources from across the country on an as-needed basis. The Coordinator would draw on these resources in coordination with local Managers of Operations and provide financial resourcing for these initiatives from an assigned unit budget.

c) Operations

Exhibit VII-4, below, represents a high-level "generic" description of how field operations would be organized. The model would have to be modified somewhat in each area of the country in order to accommodate the size and complexity of services provided.

Exhibit VII-4
Field operations


Federal Services
Economic Crime Branch
Manager(s) (Operations) Region/Division
Team Coordinator(s) (Div'n/Sub Div'n/Detachment)
Admin/Technical Support
Investigative Support
Accounting Support
Legal Support
Forensic Analysis Support
Operational Team
Operational Team
Operational Team

- Vision and strategic direction
- Overall program mgt and control
- International liaison
- Intake of investigation requests

- Mgt & control of reg'l/div'l program
- Budgeting and operational planning
- Intake of investigation requests

- Participate in operational planning and budgeting
- Intake of investigation requests
- Allocate resources to operational teams
- Coach/advise teams
- Coordinate support requirements
- Evaluate performance
- Liaise with other Coordinators
- Conduct complex investigations
- Public & client/partner education/liaison

- Clerical/admin support
- Informatics support

- Provide CIS support
- Provide forensic accounting support to investigations
- Advise on Case Law
- Work with investigative teams as assigned
- Prepare for court, present and close file

- Receive/investigate complaint /information re: offence
- Review and assess data
- Prepare operational plans re: cases, target areas, etc.
- Collect and analyze evidence
- Apprehend and process suspects
- Prepare for court, present and close file
- Gather intelligence
- Participate in community liaison efforts

(Tech Crime Investigators would occupy designated and funded positions and form Operational Teams working on computer as well as computer-assisted economic crimes)

i) Manager of Operations

Managers of Operations would exist at either the regional or divisional level depending on the size of the region/division. These managers would be drawn from current OICs/NCOs of existing Commercial Crime Sections would report directly to the Head of the National Economic Crime Program and maintain overall responsibility, authority and accountability for the management and control of the day-to-day operations in the field. They would work very closely (as a management team) with the Head of the National Economic Crime and the Policy and Program Development Centre Managers to develop and implement the national Economic Crime strategy, national standards of service, operational guidelines and criteria for service delivery, to ensure consistency across the country. This management team would also focus on the development and enhancement of partnerships/relationships with national and international stakeholders, and the establishment and maintenance of a continuous learning and development environment within the Program.

As well, Managers of Operations would work closely with their own Team Coordinators within the region/division to plan and implement their portion of the national program. They would have assigned human and financial resources with full budgetary control for their operations. Their performance measurement would be based on goals and objectives set out in conjunction with the Head of the National Program, and as identified in Program strategic and business plans. Managers would have full authority within their budgetary control and be held accountable for proactively managing ongoing operations and meeting agreed expectations. These Managers would also assume responsibility at the local level for ongoing liaison and coordination with CROPS officers and regional/divisional Commanding Officers.

Along with the Head of the National Economic Crime Program and the Policy and Program Development Centre Manager, Managers of Operations would facilitate partnerships/relationships with stakeholder groups on a local, national and international level, develop and implement operational practices and processes, etc., in conjunction with their Team Coordinators. Operational Managers and Team Coordinators would work together regarding the intake, selection and priorization of cases in line with national requirements.

ii) Team Coordinators and Operational Teams

Team Coordinator

The position of Team Coordinator would exist at the Division, Sub-Division or Detachment level depending on the size and the local configuration of each field area. The number of Team Coordinators would differ depending on the number of investigators within the local area. The span of control of Team Coordinator to investigator should represent a ratio of approximately seven to ten investigators reporting to one Team Coordinator.

Team Coordinators would provide local leadership and management to assigned operational teams of investigators. In larger divisions/regions where Economic Crime Program activities are more specialized in nature, the Team Coordinators would head up Operational Team(s) comprised of investigators in a particular specialization (e.g., markets and securities, tech crime, etc.). In smaller regions/divisions, Team Coordinators would be responsible for multi-disciplinary teams comprised of investigators working on cases in a variety of areas (e.g., fraud, bankruptcy, counterfeiting, etc.).

Team Coordinators within a local area would work closely with their Managers of Operations regarding operational planning and budgeting, intake of cases, etc. As well, the local Team Coordinators would need to work together as a management team to ensure appropriate allocation of resources (financial and human) to cases, the selection and priorization of cases, and the monitoring of performance. Team Coordinators would have appropriate budgetary authority and be held accountable by Managers of Operations to operate within assigned budgetary constraints.

As well as being responsible for the allocation of assigned resources to individual cases, Team Coordinators would act as leaders and coaches/mentors and even expert investigators to assigned operational teams. They would coordinate investigational support requirements, assign cases, and evaluate performance of assigned resources. They would also play a major role in such proactive services as increased stakeholder/public awareness and education regarding Economic Crime focusing on prevention and deterrence. They would participate on joint task forces, in industry associations, as conference/meeting speakers, etc., to ensure coordination of efforts amongst all key players.

Operational Teams

Operational Teams would be comprised of investigators who specialize in certain areas (e.g., markets and securities, tech crime, etc.) and/or investigators working in a number of areas of economic crime. The composition of these Operational Teams would be flexible depending on local needs, the variety of cases within a locality, and the requirement for specialized groups of investigators within a particular field area. Operational Teams comprised of both senior and junior investigators would be responsible for the ongoing investigation of cases. These teams would work closely with their Team Coordinators to evaluate and priorize cases and conduct investigations. Investigators would also participate in liaison with and education of clients/stakeholders and their communities to enhance awareness and prevention of crime.

Tech Crime operational teams

Tech Crime investigative teams would be formed within a local program area depending on need. These investigators would occupy officially designated and funded Tech Crime positions and assume primary responsibility for the conduct of computer crime investigations (e.g., focused on hacking/unauthorized use of computer, mischief to data, and theft of telecommunications, etc.) occurring in a specific location. The Tech Crime investigators would also provide investigative support and technological expertise to other investigators on computer-assisted crimes within the Economic Crime program.

Support to other Crime programs would be provided by High Tech Crime Forensics in Ottawa or through negotiated agreement between the Tech Crime Policy and Program Development unit in Economic Crime and those programs requesting assistance. At present since no agreements exist, other crime programs have no motivation to estimate/forecast the amount of assistance they would require over a given time period. Setting up a more formal "agreement" structure, would require other programs to do more formal forecasting of their needs and would allow Tech Crime to obtain and maintain more accurate data concerning assistance provided and justify any resource adjustments which may be required to continue such support. Consistent formal monitoring of this support (e.g., time applied, types and levels of complexity of cases, type of support provided, etc.) would be done and reported regularly to the Tech Crime Policy and Program Development unit at Headquarters in order to support future decision-making as to the optimal organizational configuration of Tech Crime in the medium and long-term.

iii) Operational Support

The Operational Support side of the field operations structure is comprised of administrative and technical support, as well as more specialized investigative support.

Administrative and Technical Support

Administrative support would be required at two levels. At one level would be the requirement for a pool of administrative resources focused on providing clerical, secretarial, and word processing support to the local unit.

In addition to this support, there would also be a requirement for a higher level of administrative support to assist Team

Coordinators and Operational Teams in setting up investigation files, cataloguing evidence, maintaining case files, conducting background research, etc. to free up investigators to concentrate on more in-depth and technical investigative duties.

As well, there would be a requirement for Informatics Services to support the Program's in-house systems. This technical support could be provided as part of the FTE complement of the local Program unit or could be a shared support service with other local program units within a region/division.

Computer Investigative Support

Computer Investigative Support (CIS) is highlighted as a critical support requirement due to the increasing use of technology as the medium for the commission of economic crimes. Hands-on Computer Investigative Support (CIS) teams would report to Managers of Operations and provide more in-depth forensic analysis and technical support to all investigators within the local Economic Crime Program units.

Flexibility would be required in setting up CIS services because of differing levels of need for these services. In the Central region, two teams might be required to provide services to Ontario and Québec individually due to language requirements as well as a volume of investigative activities.

CIS teams would be a reactive operational function involved in providing support to Economic/Tech Crime investigations, trouble-shooting, providing specific information technology expertise and in-depth forensic analysis capability, as required. In smaller regions, sharing CIS resources between divisions and even regions could provide opportunities for some economies of scale.

If the CIS services provided by these units were required by other programs, some type of service level arrangement would need to be developed to provide these services. As with Tech Crime investigator time, CIS services would be provided through these negotiated agreements. Consistent formal monitoring of this support (e.g., time applied, types and levels of complexity of cases, type of support provided, etc.) would be done and reported regularly to the Tech Crime Policy and Program Development unit at Headquarters in order to maintain accurate data to support future decision-making as to the optimal organizational configuration of Tech Crime in the medium and long-term.

Specialized investigative support

Forensic accounting services and legal support services could be provided in a variety of ways depending on the differing needs across the country. If a particular Manager of Operations and his/her Team Coordinators saw an ongoing need for forensic accounting and legal support services because of the complexity and volume of their caseload, such services could become part of the permanent complement of the unit within the assigned salary envelope.

However, serious consideration should be given to obtaining these services on a contractual basis. More senior expertise can be obtained this way on a time applied basis, with ongoing support and additional specialization, as required, provided by the contractor's home organization.

A more detailed list of sub-activities required by the Program is provided in Appendix E to this report.

D. Evaluation of National Economic Crime Program Model against organization design principles

1. Business orientation

The recommended option focuses squarely on the delivery of the Economic Crime mandate. It focuses on core business activities in the framework of an overarching national strategy for Economic Crime. As a national program, it provides a level of standardization and consistency in service standards and business practices which is missing at the present time. The model also focuses on the delegation of responsibility and authority of the appropriate managerial and working levels and provides for the establishment of commensurate expectations to ensure accountability at all levels.

2. Flexibility

The recommended National Program model establishes a forward-looking functionality in the Policy and Program Development Centre focused on analyzing trends and issues and planning for the future. A national program will also be able to respond to major case requirements more efficiently and effectively on a national basis, as well as ensuring greater sharing of information and deployment of Program staff to meet ongoing and special needs. This model provides the greatest flexibility by being able to respond to local needs (through co-location of operational resources) while still being able to provide a consistent and coordinated response to broader national and international requirements.

3. Customer focus

From a regional, national and international customer perspective, the recommended model provides a cohesive, consistent and coordinated response to Economic Crime customer needs. The model fosters a more empowered and proactive approach to partnering with clients and stakeholders. It facilitates greater awareness at all levels through a focus on increased liaison, education and prevention.

From a Tech Crime perspective it maintains a more narrow customer focus by retaining Tech Crime within Economic Crime in support of the current mandate. Provision of ongoing Tech Crime support to other programs, at least over the short-term, would require the establishment of mechanisms such as service level agreements and commensurate support requirements to address historical concerns.

4. Employee development

The recommended model promotes a flexible and empowered staff complement with the appropriate level of resources to "do the job" along with the commensurate levels of authority and accountability required. To maintain ongoing effectiveness, the model requires competent employees with the required skills and abilities.

Implementation of the model would require a commitment to fund and staff all allocated positions and provide appropriate levels of both learning and development and technology support tools to position incumbents to carry out their duties effectively.

As a national program, the model also provides greater opportunities for transfers, secondments, rotation of staff through headquarters and positions in the field, to promote the development and maintenance of employee skill levels.

5. Efficiency and effectiveness

The recommended model provides the greatest opportunity for enhanced efficiency and effectiveness on a national basis. Policy and Program Development and Operations report within the same structure thereby fostering clearer and more direct communications and less fragmentation of authority and accountability. As well, fewer organizational layers allow for enhanced empowerment and flexibility of both management and operational teams.

6. Implementation

From an implementation perspective, the recommended model will require more effort to implement successfully than maintaining the status quo. A focused and detailed implementation plan will be needed to highlight the benefits of a National Program and market this approach to all decision-making levels. The model will meet with both resistance and support: resistance from those who would like to maintain the status quo/who fear a loss of power base; and support from Economic/Commercial Crime members demoralized by the current program status and frustrated and angry Stakeholders who see no consistent and comprehensive national service delivery and customer focus.

E. Rationale for moving to a National Economic Crime Program

When making a major organizational change, building a "case for change"—identifying why the organization needs to change/the benefits to be accrued from such a shift should be stated. In this section, we outline some reasons for/benefits of moving to a National Economic Crime Program model.

Economic Crime

1. Stakeholders and Members stress a national focus

Both Stakeholders and Members of the current Economic/Commercial Crime program stressed a need for a national strategy and direction to address economic crime activity across Canada.

A national program model facilitates more effective control over and management of adequate national programming and resourcing. It focuses on key business activities by establishing a consolidated, cohesive and proactive approach to federal economic crime investigation, education, and prevention. The model allows the Program to more effectively:

- Plan for the future.
- Share information/intelligence/best practices.
- Develop and maintain continuous learning.
- Consolidate resources to address major national requirements, and obtain specialized expertise (e.g., technology, forensic accounting, legal, expertise, etc.).

- Rotate staff between Headquarters and the field.

2. The need for a "national" community policing model

The National Program model recommended supports and complements the Force's commitment to community policing. For the RCMP as a national police force, community policing must occur at least two levels—one being the local level (both provincial and/or municipal in contract provinces), and the other at the national level.

At the local level, focus must be on keeping our streets and homes safe. However, at the macro level we also have the national community of our country. As citizens of Canada, we must be assured that our national community is also being protected from those who want to corrupt our systems and infrastructures and perpetrate crimes against both individual citizens and our institutions. As a national Police Force, the RCMP must take responsibility for working with local policing authorities to protect local communities but must also focus its effort on protecting our national community. As a national community, we must survive in an era of increasing globalization, with risks not only at the local level but even more so at the national and international level. A National Program to address economic crime performs just such a function.

3. Canada is perceived as a safe haven for organized crime

A national program model allows Economic Crime to focus effort on its mandate—to address organized crime which is now operating on a more national and international basis and becoming more and more technologically sophisticated.

The current lack of such a national approach puts Canada increasingly at risk of not being able to address the growth in economic crime from both national and international sources and increases Canada's profile as a safe haven for organized crime. No longer can we allow multi-jurisdictional cases to fall between the cracks. A national approach will allow more effective marshalling of resources both nationally and with our international neighbours.

4. Politicians commit to increased international partnering

As the world becomes smaller, our political leaders become more aware that it is impossible for Canada to fight economic crime in isolation. Few countries have inexhaustible resources to fight economic crime as it transcends borders and affects all segments of society. To that end, senior political ministers from all countries meet regularly to establish agreements to cooperate and coordinate forces to respond to these threats. The political will to increase international partnering in the fight against economic crime requires a program national in scope to be able to respond effectively. International partners are looking for a single point of contact here in

Canada and an effective decision-maker represented around the table where these agreements are forged. A national program can provide just such a single point of contact supported by a myriad of skills and knowledge.

5. Economic Crime must support addressing systemic Human Resources Management problems

As indicated previously, the current Economic/Commercial Crime configuration is facing a number of systemic Human Resources Management (HRM) problems including: attraction, recruitment, and retention of qualified staff; career pathing and succession planning; the promotional process; and high turnover/ongoing attrition.

As a national program, Economic Crime would be better positioned as a united voice to support addressing these current as well as any future HRM issues in an expeditious manner.

6. A more flexible management model is required

At present, both stakeholders and members indicate a lack of leadership and effective management practices in the current Economic/Commercial Crime programs. Commercial Crime Sections are subject to the changing needs of the local management structure with little or no control over either financial or human resources. Delivering on the national mandate is currently heavily influenced by regional priorities. Federal positions are often sacrificed to support provincial priorities and/or to address budgetary shortfalls.

The Economic Crime Branch in NHQ has little or no say in the allocation of resources because it has no funding authority. This situation renders the Branch "toothless" when it comes to providing national leadership and direction and ensuring national standards of practice and consistency in service delivery.

A national program would in essence put more "control of their own destiny" into the hands of both Headquarters and field staff.

7. Implementation considerations

The most important consideration if the National Economic Crime Program model were implemented, is the funding formula. There are two potential funding options presented below.

Option 1

The first option would be for the new Program to absorb all current federal positions located within the Economic Crime Branch at NHQ and throughout all Commercial Crime Branches and Sections across the country, along with any additional resources obtained. The provincial positions would remain in the regional structure and could be combined with GIS sections for reporting purposes or form standalone units. These positions would focus on provincial cases.

Although this funding option would provide the least disruption of provincial agreements currently in place, it is not the optimal solution. Leaving the provincial positions within the regional structure would not address any of the leadership, managerial, skills and resource allocation issues raised by national and echoed by provincial Stakeholders. These positions would have little access to ongoing learning and development and the required technology support tools. They would have to be supported in some way by the National Economic Crime program in order to ensure at the very least, a skilled and competent resource pool from which to draw for the National Program.

Option 2

The second option provides a more optimal funding solution. In this option, all positions, both federal and provincial, currently in the Economic Crime Branch and the Commercial Crime Branches and Sections would be transferred to the National Economic Crime Program, along with any additional resources obtained. The Program would then establish a charge-back formula in accordance with current provincial requirements in order to continue to meet provincial needs. Percentage charge-backs would likely differ somewhat from province to province depending on the established level of service. In essence, provinces would still be funding and obtaining services for provincial cases but the National Program would retain the flexibility of assigning appropriate staff to the jobs.

The status quo situation where provinces fund specific positions within Commercial Crime sections program could be maintained until provincial agreements come up for re-negotiation. However, during the re-negotiation process or before, if possible, the National Economic Crime Program should lobby for the provision of an agreed level of service versus the actual delineation of particular positions as provincial. This would afford the Program greater management flexibility in the long-term.

As well, by using this formula, all Program members and support services would be included in continuous learning and development programs, partnering with external stakeholders, proactive awareness and prevention initiatives, and regular upgrading of technological support tools. The provinces would continue to receive the same level of service and would benefit from working with investigators who have excellent skills and competencies in the field of economic and technological crime. Any requirement for additional services by provinces would have to be negotiated with the National Program.

Tech Crime

Over the course of the study, much discussion took place regarding Technological Crime, what it encompasses as well as how it should be structured to deliver services. As indicated in the report on Tech Crime (Deliverable #3), Tech Crime was defined as including both crime where the computers/systems or their contents are the targets of the offence, and computer-assisted crime where traditional crimes are facilitated by the use of computer technology.

In deciding on an organizational configuration for Tech Crime, KPMG debated regarding whether to recommend Tech Crime remain as a service line within the National Economic Crime Program or to recommend setting up Tech Crime as a separate Federal Services program. Within the current Economic/Commercial Crime structure, there are two schools of thought on this topic—one supports the retention of Tech Crime within a National Economic Crime program and the other supports a separate program.

We listened to both sides of the debate and also gleaned opinion external to the program and the Force. Though there are, of course, advantages and disadvantages to both models, at this time KPMG recommends retaining Tech Crime within the National Economic Crime Program. At a future date, should Tech Crime achieve an increased resource base and be able to establish a viable infrastructure, a separate national Tech Crime program may be the optimal solution. At present, we do not feel that such a structure is viable. Below we provide some reasons why we support keeping Tech Crime within the Economic Crime Program.

1. Insufficient critical mass currently exists

At present approximately 34 FTEs are working in the Tech Crime area across the country. Only about 24 of these FTEs are actually occupying designated/funded positions. Insufficient critical mass at this time does not make it viable to set up a separate national service line complete with the required infrastructure to support 30+ individuals. Infrastructure including administrative and technical support would be required across the country and this would not be a good use of limited resources. Otherwise, the service line would have to share infrastructure support with either the decentralized operations or with a specific program and contribute to the sharing of those services.

2. Tech Crime infrastructure already exists in Economic Crime

Through anecdotal report only, many Tech Crime investigators indicate that they spend time providing services to other crime programs. However, little formal tracking of this information is done to determine what type and how much support is being provided. As well, little information is available regarding the current level of technological skill residing in other crime programs. Since an infrastructure for Tech Crime already exists in Economic Crime, this infrastructure could be enhanced for either the short or longer term to coordinate Tech Crime activities across the country in a more cohesive manner, establish more of a trend research and analysis base, and establish mechanisms to capture workload and performance data in a more formal and reliable manner.

3. Tech Crime is part of the Economic Crime mandate

The responsibility for Tech Crime is an integral part of the current Economic Crime mandate. This mandate was developed and reviewed over a significant period of time and agreement and approval of both Management was obtained. While removing Tech Crime responsibility could be done, another modification and approval process would be required.

4. The interim

For at least the interim, Tech Crime should remain within the National Economic Crime Program—as a national line of service. This will allow Tech Crime to organize for the future. During this period, Tech Crime can address the following needs:

- Clarify what the definition of Tech Crime encompasses, what the mandate of Tech Crime should be, and what direction Tech Crime should establish for the present and the future.
- Develop formal performance measurement mechanisms to obtain a better understanding of both workload activity and performance data, e.g.,:
    - Percentage of time spent on Tech Crime cases.
    - Creation of dedicated Tech Crime financial tracking codes to measure workload activity.
    - Definition of types of Tech Crime, levels of complexity, etc.
- Designate and fund required positions.
- Examine overlaps with other Federal Service programs and establish mechanisms to coordinate services and/or merge services over time depending on feasibility.

- Conduct cost benefit/impact analysis of consolidating High Tech Crime Forensics (HTCF) and any other overlapping technology-oriented areas (e.g., software piracy, etc.) with Tech Crime.
- Establish appropriate level of CIS support required in Tech Crime.
- Establish mechanisms/methods to address upgrading basic technology skills of all investigators within the Economic Crime Program and determine upgrading requirements for other Federal Services programs.
- Verify future feasibility of establishing Tech Crime as a distinct/separate service line within Federal Services.

F. Skills and competencies

To carry out an efficient and effective National Economic Crime Program, the following skill sets for each component of the Program have been identified as minimum requirements for success. Some of these skill sets are very specialized/technical in nature. Although necessary to support effective functioning of the Program, the most practical way of obtaining some very specialized skills and knowledges (e.g., technological expertise, forensic accounting expertise, legal expertise, etc.) may be through partnering with Industry, other agencies, or even outsourcing to obtain the expertise on an as required basis.

1. Suggested overall basic requirements

We have recommended that the National Economic Crime Program be defined as a specialized program requiring specialized skills. If this is indeed the case, some minimum requirements should be established to guide recruitment and selection of individuals for the Program as well as for progression within the Program.

In establishing any type of minimum recruitment and selection criteria, a measure of flexibility must be maintained. Selection is not a black and white process. Sometimes, the best candidates do not meet all the requirements fully but still may have great potential to be excellent Economic Crime investigators. Therefore, it will be critical not only to establish some minimum selection requirements to use as a baseline, but also for the Program to work very closely with the staffing function to apply these requirements but still remain flexible enough to consider those individuals who show promise and may meet perhaps only 80% of the criteria.

No effective recruitment process can rely solely on rigid minimum requirements. Tempering these baseline requirements with the critical and ongoing input and decision-making of line/operational managers within the Program is key to an effective staffing/recruitment process.

Historically, recruitment into the RCMP required no more than a high school diploma. Recruits came into the Force at an average of 18-20 years. Although this historical situation still exists to some extent, the average age of recruits to the Force has increased to approximately mid to late 20's. In essence this means that most individuals coming into the Force have either a spent more time increasing their educational level or working in another field such as industry, the public sector, etc. This translates into a base level of formal skills and knowledge as well as life experience which is higher than in the past and consequently of potentially more interest to and applicability for the National Economic Crime Program. Therefore, the Program should be able to recruit cadets/identify cadets for recruitment right out of the Cadet academy. Setting a baseline of requirements to be applied flexibly would aid in the identification and selection process.

Requirements for recruiting cadets would be set out as:

- A university/community college degree in Business Administration or related area (e.g., economics, criminology, law) **or** for Tech Crime—a computer science/systems engineering degree/diploma.

- 1-3 years of industry experience (e.g., stock market/brokerage, financial institution, business sector, high tech industry, etc.) of direct applicability to the Program.

OR

- 4-5 business-related courses (e.g., cost accounting, management accounting, business law, securities courses, economics, etc.)

- 3-4 years of related business/industry experience.

Hands-on investigative techniques would have to be learned on the job.

Requirements for recruiting from other areas of the Force

For those members who are already in other RCMP programs, the experiential level with accompanying investigative experience would have to be complimented by a minimum number of business-related courses and the agreement to pursue further study/skills upgrading to show an ongoing interest in and commitment to the Program. A baseline requirement for these types of candidates should parallel somewhat the recruitment/selection criteria for candidates from the Cadet academy.

- 4-5 business-related courses (e.g., cost accounting, management accounting, business law, securities courses, economics, etc.).

Having these courses successfully completed at either a university or community college level would indicate both aptitude for and interest in Economic Crime on the part of the Member.

AND

- 3-4 years RCMP experience preferably in another program using investigative skills and techniques or in combination with related industry experience.

As well, candidates transferring from other RCMP programs with the minimum formal course requirements listed above, should agree to continue upgrading their formal education qualifications either by completing a degree or diploma and/or taking additional specialty certification (e.g., advanced securities training, etc.) while in the Program.

Progression/promotion

For progression/promotion within the National Economic Crime Program, criteria should be based not only on the baseline requirements set out above, but also on an indication on the part of an individual investigator to a commitment to ongoing skills and knowledge upgrades, and increased experiential levels/evidence by way of on-the-job experience, of an ability to perform. For example:

- Conduct of increasingly more complex investigations.
- Ability to plan and execute plans effectively.
- Ability to take initiative and assume more responsibility not only for self management but also team and case/project management.
- Ability to manage within budgetary constraints.
- Ability to delegate tasks and authority and mentor junior/new members.
- Ability to lead.
- Ability to manage more than one task effectively at one time, etc.

As well, the Program may want to use a minimum number of years at a particular level as a rule of thumb prior to considering an individual for progression through the Program. Such a rule of thumb used by most project-oriented organizations is a minimum of 2-3 years at a certain level to obtain a broader spectrum of experience.

Instituting a very rigid set of educational and/or experiential criteria for progression/promotion would in fact tie the hands of managers and prevent them from being able to reward individuals for superior/effective performance.

A more detailed list of skills and competencies for key types of positions is provided below.

a) Program Head Economic Crime Branch

Knowledge

- Good understanding of all Economic Crime areas.
- Familiarity with business principles and practices. Commitment to ongoing skills and knowledge upgrades.
- Comprehensive knowledge of current and future trends and issues.

Competencies/skills

- **Leadership skills**—strategic perspective, strategic thinking, analytical thinking, strong orientation to change, interpersonal sensitivity, excellent communications skills, decisiveness, creates a learning environment, gains commitment, motivating, leveraging diversity, relationship building.
- **Management skills**—goals/results oriented, coaching/ mentoring, directing, developing people, planning, cost sensitivity, initiative, innovation business acumen, managing performance, customer focus, environmental sensitivity.

b) Manager Operations

Knowledge

- Comprehensive understanding of all Economic Crime areas.
- Good understanding of business principles and practices. Commitment to ongoing skills and knowledge upgrades.

- Good knowledge of current and future trends.

Competencies/skills

- **Leadership skills**—tactical perspective, analytical thinking, strong orientation to change, interpersonal sensitivity, excellent communications skills, decisiveness, creates continuous learning environment, motivating, relationship building, collaborative, leveraging diversity, gains commitment.
- **Management skills**—proactive, results-oriented, coaching, mentoring, developing people, tactical planning, initiative, innovative, cost sensitivity, business acumen, managing performance, customer focus.

c) Team Coordinator

Knowledge

- Comprehensive understanding of all Economic Crime areas.
- In-depth understanding of one or more specialty areas.
- Good understanding of business principles and practices. Commitment to ongoing skills and knowledge upgrades.
- General understanding of technology and office automation software.
- Good knowledge of current and future economic crime trends.

Competencies/skills

- **Leadership skills**—analytical thinking, operational perspective, excellent communications skills, motivating, collaborative, gains commitment, promotes teamwork.
- **Management skills**—proactive, results-oriented, coaching, mentoring, directing, developing people, team planning, maximizing performance, managing performance, customer focus.
- Excellent investigative skills.

d) Economic Crime Operational Teams

Knowledge

- Good understanding of business principles through formal education and/or industry/business experience.
- In-depth understanding of one or more specialty areas.
- General understanding of technology and office automation software.
- Good understanding of policies & procedures for dealing with technology used in commission of crimes and how electronic data could be used as evidence. (Understanding of operating systems—what they can/cannot do, when to touch the computer and when to call in more technological expertise, etc.).

Competencies/skills

- Excellent investigative skills.
- Initiative.
- Good interpersonal skills.
- Good communications skills.
- Collaborative.
- Self-directed learner.
- Team player.
- Self-motivated/self-starting.

e) Tech Crime Operational Teams

Knowledge

- Excellent investigative skills.
- A computer science/systems engineering background (at a minimum, computer science courses preferably at the University level or at the Community College level)—intermediate level knowledge of operating systems (Unix,

Linux, etc.), the Internet, voice and data communications data retrieval methods, hardware configuration, etc.

- Forensic analysis capability.

Competencies/skills

- Excellent investigative skills.
- Initiative.
- Good interpersonal skills.
- Good communications skills.
- Collaborative.
- Self-directed learner.
- Team player.
- Self-motivated/self-starting.

f) Investigative Support

Computer Investigative Support teams

Computer Investigative Support (CIS) teams located in the regions/divisions would provide reactive forensic analysis and media technical support services to investigative teams. These teams would be established from a pool of investigative support personnel with a variety of technical expertise. Not all skills would necessarily be resident in all teams. Technical expertise could be assigned in accordance with volume and types of crime in a particular region. Resources could also be shared between regions. Skill sets required would include:

- Formal computer science/systems knowledge (certification in/or more technical areas: operating systems, hardware configurations, utilities, database expertise, etc.)
- Systems engineering knowledge (voice & data communications, internal computer processing, etc.)
- Forensic analysis skills.
- Good investigative skills.
- EDP audit skills.

Because this field is highly technical requiring a variety of technical expertise, this area would be a prime location for optimizing partnering solutions. In addition to in-house expertise in CIS, obtaining expertise from the High Tech industry, Information Technology consulting firms, should be explored. Setting up a pool of experts from which CIS teams can draw will provide a rapid response mechanism based on need. To reduce costs for such partnering, the Tech Crime Policy and Program Development unit should explore the possibility of sharing these services with other policing authorities.

Administrative Support

- Clerical/secretarial skills.
- Research skills.
- Analytical skills.
- Organizational skills.
- Data entry skills.

Specialty Support

Because this area requires such specialized skill sets, this would be a prime location for optimizing partnering and/or outsourcing solutions. As with CIS, setting up a pool of experts from which different field areas can draw will provide a rapid response mechanism.

- Legal skills.
- Forensic accounting skills.

g) Policy & Program Development

Knowledge

- Comprehensive understanding of Economic Crime areas.
- In-depth understanding of one or more specialty areas (e.g., markets and Securities, Tech Crime, etc.).
- Good understanding of business principles and practices. Commitment to ongoing skills and knowledge upgrades.
- Comprehensive understanding of technology.

- Excellent knowledge of current and future trends.

Competencies & Skills

- Proactive, multi-disciplinary units.
- Conceptual thinking (policy development, standards of practice, etc.)
- Forward thinking (modelling, forecasting, trend analysis, etc.)
- Systematic/analytical thinking skills (logic, problem-solving, cause and effect analysis, etc.)
- Statistical skills (maintenance of data repository, support to research and trend analysis).
- Audit and evaluation skills.
- Change management/business administration skills (restructuring, redesigning, planning and monitoring, communications, facilitation).

VIII

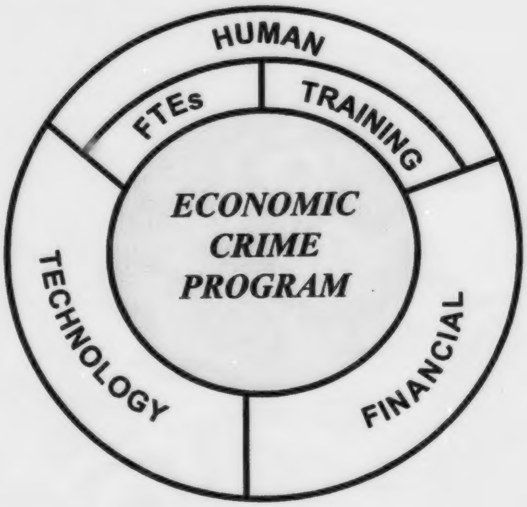
Resource Issues And Requirements

This chapter discusses the resources that are integral to the Economic Crime Program and issues regarding how they are and should be managed. It also identifies the management, investigator and support positions required to meet the mandate.

A. Economic Crime Program resources

In order for the Economic Crime Program to meet its mandate and the emerging challenges discussed in previous chapters, it must have sufficient resources. Human, financial and technology resources are critical for the program, as depicted in Exhibit VIII-1.

Exhibit VIII-1
Resources for the Economic Crime Program



The Program must have the right mix of manager, investigator and support resources, and these resources must receive appropriate training to stay at the leading edge of the field. Investigators, in particular, those in the Tech Crime area, must have the right equipment to be effective. Sufficient financial resources are required to support salaries, investigation costs, technology requirements, travel, training requirements and crime prevention.

Exhibit VIII-2 shows the three-year trend in FTEs, salary and non-salary expenditures for the Economic Crime Program. The overall expenditures have remained constant overall, but there has been a decrease in both since 1996/97.

In recent years, there has not been any growth in resources for Economic Crime, due to program review. Most adjustments in resource levels have been budget reductions. It is our understanding that since Program Review I and II, the RCMP has not obtained (nor asked for) new resources for other than recognized government priorities, such as Integrated Proceeds of Crime (IPOC) and Anti-Smuggling Initiative (ASI). Hence, today's budgets and FTEs (with the exception of special initiatives) are more or less the same as they were three to four years ago when Operating Budgets were introduced in the government. Resources are allocated historically according to who predicted growth in market areas and fraud, not likely based on a rational process based on demand.

B. Overall approach to resource management

In addition to identifying what resources, and in what amounts, are required to support the program, we looked more broadly at the management of resources for the Program. Our approach was to look at four areas in resource management, as shown in Exhibit VIII-3.

Exhibit VIII-2

FTEs and Expenditures for the Economic Crime Program, 1995 -1996 through 1996 - 1997

		A Ottawa	B NFLD	C Quebec	D Man	E BC	F Sask	G NWT	H NS	J NB	K Alta	L PEI	M YT	O Ont	N Ottawa	TOTAL RCMP
1995-1996	Pay	1,726	734	6,064	1,583	4,743	1,376	252	951	732	2,896	363	186	5,484	570	27,660
	O&M	100	147	514	112	884	211	112	210	73	431	12	33	953	114	3,906
	Minor Capital	70	2	163	40	14	-	6	12	1	50	4	9	51	1	423
	Total O&M	**170**	**149**	**677**	**152**	**898**	**211**	**118**	**222**	**74**	**481**	**16**	**42**	**1,004**	**115**	**4,329**
	Major Capital	-	-	-	-	86	19	-	38	-	57	-	-	77	-	277
	TOTAL $(000)	**1,896**	**883**	**6,741**	**1,735**	**5,727**	**1,606**	**370**	**1,211**	**806**	**3,434**	**379**	**228**	**6,565**	**685**	**$ 32,266**
	FTEs RM	27	11	98	26	75	22	3	15	11	48	6	3	88	9	442
	PS	2	2	11	4	8	4	0	2	2	6	1	0	8	3	53
	TOTAL FTEs	**29**	**13**	**109**	**30**	**83**	**26**	**3**	**17**	**13**	**54**	**7**	**3**	**96**	**12**	**495**
1996-1997	Pay	1,865	661	6,727	1,420	5,111	1,496	147	979	702	2,916	376	82	5,552	674	28,708
	O&M	552	162	512	121	975	257	78	205	141	544	30	11	535	117	4,240
	Minor Capital	27	3	161	54	23	89	-	-	24	40	4	-	337	15	777
	Total O&M	**579**	**165**	**673**	**175**	**998**	**346**	**78**	**205**	**165**	**584**	**34**	**11**	**872**	**132**	**5,017**
	Major Capital	-	-	-	16	17	33	-	-	-	-	-	29	19	-	114
	TOTAL $(000)	**2,444**	**826**	**7,400**	**1,611**	**6,126**	**1,875**	**225**	**1,184**	**867**	**3,500**	**410**	**122**	**6,443**	**806**	**$ 33,839**
	FTEs RM	29	10	103	23	81	23	2	16	11	47	6	1	87	12	451
	PS	2	2	13	3	10	4	-	2	3	6	1	-	9	1	56
	TOTAL FTEs	**31**	**12**	**116**	**26**	**91**	**27**	**2**	**18**	**14**	**53**	**7**	**1**	**96**	**13**	**507**
1997-1998	Pay	1,731	716	5,720	1,238	5,050	1,324	169	945	711	2,585	377	70	5,499	804	26,939
	O&M	309	133	523	243	1,066	166	80	195	131	923	27	99	741	128	4,764
	Minor Capital	45	3	50	13	250	6	-	8	33	229	20	6	140	43	846
	Total O&M	**354**	**136**	**573**	**256**	**1,316**	**172**	**80**	**203**	**164**	**1,152**	**47**	**105**	**881**	**171**	**5,610**
	Major Capital	-	-	-	15	39	-	-	-	-	-	17	-	-	-	71
	TOTAL $(000)	**2,085**	**852**	**6,293**	**1,509**	**6,405**	**1,496**	**249**	**1,148**	**875**	**3,737**	**441**	**175**	**6,380**	**975**	**$ 32,620**
	FTEs RM	28	11	90	20	80	21	2	15	11	41	6	1	84	12	422
	PS	2	2	9	3	10	4	-	2	2	7	1	-	8	3	53
	TOTAL FTEs	**30**	**13**	**99**	**23**	**90**	**25**	**2**	**17**	**13**	**48**	**7**	**1**	**92**	**15**	**475**

Source: Planning and Budgeting section.
"RM" denotes "regular members", "PS" denotes "public servants".

Exhibit VIII-2

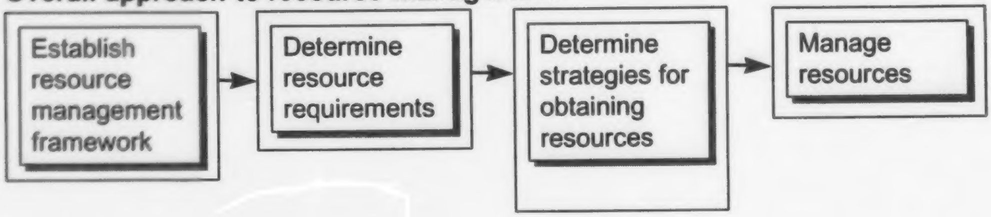
FTEs and Expenditures for the Economic Crime Program, 1995 -1996 through 1996 - 1997

		A Ottawa	B NFLD	C Quebec	D Man	E BC	F Sask	G NWT	H NS	J NB	K Alta	L PEI	M YT	O Ont	N Ottawa	TOTAL RCMP
1995-1996	Pay	1,726	734	6,064	1,583	4,743	1,376	252	951	732	2,896	363	186	5,484	570	27,660
	O&M	100	147	514	112	884	211	112	210	73	431	12	33	953	114	3,906
	Minor Capital	70	2	163	40	14	-	6	12	1	50	4	9	51	1	423
	Total O&M	170	149	677	152	898	211	118	222	74	481	16	42	1,004	115	4,329
	Major Capital	-	-	-	-	86	19	-	38	-	57	-	-	77	-	277
	TOTAL $(000)	1,896	883	6,741	1,735	5,727	1,606	370	1,211	806	3,434	379	228	6,565	685	$ 32,266
	FTEs RM	27	11	98	26	75	22	3	15	11	48	6	3	88	9	442
	PS	2	2	11	4	8	4	0	2	2	6	1	0	8	3	53
	TOTAL FTEs	29	13	109	30	83	26	3	17	13	54	7	3	96	12	495
1996-1997	Pay	1,865	661	6,727	1,420	5,111	1,496	147	979	702	2,916	376	82	5,552	674	28,708
	O&M	552	162	512	121	975	257	78	205	141	544	30	11	535	117	4,240
	Minor Capital	27	3	161	54	23	89	-	-	24	40	4	-	337	15	777
	Total O&M	579	165	673	175	998	346	78	205	165	584	34	11	872	132	5,017
	Major Capital	-	-	-	16	17	33	-	-	-	-	-	29	19	-	114
	TOTAL $(000)	2,444	826	7,400	1,611	6,126	1,875	225	1,184	867	3,500	410	122	6,443	806	$ 33,839
	FTEs RM	29	10	103	23	81	23	2	16	11	47	6	1	87	12	451
	PS	2	2	13	3	10	4	-	2	3	6	1	-	9	1	56
	TOTAL FTEs	31	12	116	26	91	27	2	18	14	53	7	1	96	13	507
1997-1998	Pay	1,731	716	5,720	1,238	5,050	1,324	169	945	711	2,585	377	70	5,499	804	26,939
	O&M	309	133	523	243	1,066	166	80	195	131	923	27	99	741	128	4,764
	Minor Capital	45	3	50	13	250	6	-	8	33	229	20	6	140	43	846
	Total O&M	354	136	573	256	1,316	172	80	203	164	1,152	47	105	881	171	5,610
	Major Capital	-	-	-	15	39	-	-	-	-	-	17	-	-	-	71
	TOTAL $(000)	2,085	852	6,293	1,509	6,405	1,496	249	1,148	875	3,737	441	175	6,380	975	$ 32,620
	FTEs RM	28	11	90	20	80	21	2	15	11	41	6	1	84	12	422
	PS	2	2	9	3	10	4	-	2	2	7	1	-	8	3	53
	TOTAL FTEs	30	13	99	23	90	25	2	17	13	48	7	1	92	15	475

Source: Planning and Budgeting section.
"RM" denotes "regular members", "PS" denotes "public servants".

i13

Exhibit VIII-3
Overall approach to resource management


Establish resource management framework
Determine resource requirements
Determine strategies for obtaining resources
Manage resources

It consists of four components:

- **Establish resource management framework**—addresses the accountability framework and the Program's overall approach to resource management. This looks at control and accountability for resource determination and usage, roles, NHQ Program and divisional managers in resource management, timing, etc.

- **Determine resource requirements**—based on the activities in the Economic Crime Program, appropriate approaches are used for estimating the resource requirements. This is discussed in a later section of this chapter.

- **Determine long term strategies for obtaining resources**—considers the available strategies for obtaining funds to support the mandated activities and services.

- **Manage resource allocation process**—considers the day-to-day management of the resource allocation process. This includes the appropriate infrastructure and to monitor that resources are being used effectively and efficiently.

1. Current resource management framework

a) Allocation and control of resources

Although the Economic Crime Branch is responsible for overall coordination of the national Economic Crime Program, the organizational and geographical structure of the RCMP introduces a formal chain of command for allocation of resources and control of investigators.

Resource allocation is integrated in the existing command relationships which, for the most part, excludes HQ Program Management. There is a defined command relationship between programs, divisions and detachments for resource allocation. There are many players in budgeting and resource allocation such as Corporate Finance, Division Commanders, Detachment Commanders, Division Program Managers, Division Criminal Operations Officers, Divisional Corporate Management, and Division Executive Committees (DEC). HQ Program Management does not play a noticeable role in resource allocation and management among these players.

Budgets and resources are allocated to and managed by division. Previously, divisions only had control of O&M budgets. When operating budgets were introduced, the divisions gained control of salary budgets and FTEs. They get the bottom line (pay, O&M and capital) and they have the responsibility to deliver in the program areas. Divisions receive budgets (largely historically based) from HQ finance as a lump sum, not by program (e.g., not allocated to sections or business lines). O&M and capital may be provided by unit, but salary dollars are provided at the division level and managed by the Division's Corporate Management Branch in order to oversee staffing and promotion at a Divisional level. Divisions get an authorized level of FTEs for Commercial Crime largely based on historical amounts.

Divisional budgets may then be partitioned into detachment or unit budgets for O&M, minor capital and overtime, again, primarily based on historical trends (salary is maintained at the Division level). These can be further broken down into section budgets, e.g., Commercial Crime, Drugs, but the resources are under the Detachment Commander's control. Division HQ prepares budget reports for Detachment Commanders on where they stand by collator code, e.g., Commercial Crime, Drugs, etc. The Detachment Commander can then forward reports to the OICs of the different sections.

Divisional planning and staffing functions monitor resource deployment in a variety of ways. They may do daily monitoring of vacancies, available salary dollars, adequate staffing. Alternatively, they may be tasked to look at the deployment of resources through shift schedules.

Divisions feel strongly that they need the latitude to manage and control their own budgets since they are closer to the action. If the Economic Crime Program is falling short on its objectives in a Division, the Division Commanding Officer is accountable, insofar as the Division CO is accountable for delivery. The Division CO is, in this way, responsible for appropriately using the resources allocated. Division Commanders report functionally to the Regional Deputy Commissioner and to the Commissioner, as does the head of the HQ Economic Crime Program through the Director, Federal Services. The Commanding Officers are viewed as the service deliverers in the field. The Division CO has financial and legal accountability for the budget. They must manage resources so that there is not a deficit. They align the financial and human resources to meet the mandate of the

Commissioner to the satisfaction of the stakeholders and citizens. Detachment Commanders and Division Program Managers, similarly, must ensure they accomplish the desired results.

HQ Program Managers do not have access to divisional budgets (or organization charts). They do not typically get reports on O&M expenditures by the divisions. Their current role is to focus on programs, major cases, quality assurance of cases (e.g. that they have been properly done). Their role also includes satisfaction of service delivery, and ensuring that program resources have appropriate training and are aware of policies and program issues. It is our understanding that the Commissioner expects the Program Managers to monitor the programs and manage the vacancies. They should be monitoring caseload, vacancy patterns, and workload for the business line by reviewing the MIS or OSR reports on resource usage and workload and HR reports on vacancies and strength. Theoretically, they can influence resource usage through the Division Commanders.

Formal resource re-allocation of Commercial Crime resources within Divisions often occurs without the direct involvement of HQ Program management. The process for resource re-allocation within a division and its detachments may be formal, especially in larger divisions. If a detachment does not have sufficient resources with respect to other Commercial Crime units, the Detachment Commander would forward a request to the Division Commercial Crime Program Manager. The Division Program Manager would then consult with the Commercial Crime units in the detachments of the division and with the Detachment Commanders. If the units respond that they can forego a resource given their local pressures, the Division Program Manager then discusses this with the Criminal Operations Officer who then presents it to Division Executive Committee which the Division Commander chairs. In this case, the resources are moved across detachments though not changed at the program level. HQ is not directly involved in the reallocation, though they may take on a "broker" role. Division Executive Committee may also make decisions on initial resource allocations or on-going resource allocations based on needs of the detachments. Increasingly, resource reallocation is tied to a business case approach that must take into account the relocation costs (roughly $40K) per move.

Commercial Crime investigators are often assigned to investigations outside their mandated area as a result of informal resource reallocation decisions in the field. Division and Detachment Commanders often reallocate resources to operational priorities. Though they cannot shift their own Commercial Crime investigators to other areas in terms of authorized positions, they can, and do, move the people in those positions. For example, they can put an investigator on a special investigation outside of Commercial Crime for five years, but the position officially remains in Commercial Crime. They cannot easily effect the program establishments. Commercial Crime investigators, because of their high skill sets, are often reallocated to investigations outside their mandate area.

Detachment commanders must respond to a host of requirements: red serge details, VIP duties, PR events, operational matters. These could take Commercial Crime investigators away from their investigation duties. Also, they deal directly with the vacancy problems and there may be fewer investigators available than on the books and thus, must rely on all available officers. This is not a problem unique to Commercial Crime. However, it is recognized as one of the key issues in the use of Commercial Crime, and especially, Tech Crime resources.

b) Principles for resource allocation and management

Under the proposed National Service Line, the program will have increased control over financial resources. It is critical that the management and members of the Program understand and have consensus on how resources are allocated and managed. In the course of our consultations with managers and investigators in the divisional Commercial Crime Sections, we reviewed a set of principles for resource allocation and management. There was general agreement on the principles, though it was noted that there is not concordance of current practices with the principles. The principles, and how the program fares against them is summarized in Exhibit VIII-4. Complete statements of principles and implications are included in Appendix G. The establishment of the National Service line should improve the overall resource management for the Program. In light of this, we recommend that:

- NHQ Program Management develop a clear statement of objectives and ranked priorities for the Program (which are consistent with high level departmental direction). The Commercial Crime Section management should participate in identifying and assessing, collectively, the Program priorities. These statements can then be formulated in a Program Business Plan.

- Based on the priorities and objectives, budgets are developed and assigned.

- The Program Management establish a mechanism for management to discuss and agree to resource allocations and re-allocations.

- Establish mechanisms for consulting with stakeholders and clients on a regular basis to assess demand and resources required.

Exhibit VIII-4
Principles for resource allocation and management

Principles	Key Observations
Establish formal prioritization mechanisms	Resources allocated on the basis of needs vs. priorities Divisional priorities take precedence—community policing Need a statement of overall priorities for EC Program
Resources allocated in relation to priorities	Economic Crime has not been seen as a key government priority Divisions reallocate Commercial Crime resources to operational priorities Lack of prioritization of cases
Budgets linked to the organization's strategic and business plans	No program business plan indicating priorities Allocations historically based for the Department and the Economic Crime Few, if any, business plans for sections
Program management involvement in allocating and re-allocating resources	NHQ Program Management role not significant Division management drives decisions
Operating units provide input to program priorities and resource allocation	Perception that planning and resource allocation is predominately top down Commercial Crime sections have provided input on training needs and technology requirements
Reallocate resources to address emerging pressures	Federal position vacancy salary dollars are a buffer "Scooping" by higher management of funds saved by line managers—a disincentive to planning Tight budgets: concerns re: ability to resource major investigations Re-allocation of resources to other operational duties affects ongoing investigations
Open and flexible resource allocation culture	Tight control by COs and para-military culture Federal resources are the "flexibility"
Planning and allocation process responds to issues and is simple	Planning and resource allocation not perceived to be integrated Historical budgets Barriers to responding quickly to commitment of resources (BreX)
Transparent resource allocation and usage	Program Managers do not have access to divisional budgets Managers do not have real time, readily available financial information MIS information may be inaccurate
Maximize access to external funding	Fiscal framework has been used for IPOC, Anti-Smuggling Initiative Clients provide special project funding or resources for Economic Crime Concerns regarding "two-tier" service levels, and optics of "corporate sponsorship" Need good resource tracking system to support business cases Should not use resources provided for special purposes/projects on other projects/cases
Ongoing client involvement, where appropriate, in the resource planning and allocation phases	Need close working relationships with stakeholders Need to keep stakeholders/clients informed about acceptance/status of cases
Resource allocation framework must address project/ administrative activities as well as investigations	MIS focus is operational—no tracking of resources for project/policy activities Policy activities have not been integrated with overarching program objectives
Build resource management expertise	Centralizing resources requires greater expertise among Economic Crime Program and line management—including prioritization of cases, project management, financial management

c) Program accountability

The Economic Crime Branch has provided input to the Federal Services and departmental 1998/99 Business Plans. The plan identifies key pressures and strategies. However, it does not identify program resources (inputs), and program outputs or outcomes.

The NHQ program management should document key objectives for the program, resources to meet the objectives and program outputs that are measurable.

2. Strategies for obtaining resources and working with limited resources

There are a number of strategies that the Program can take to work with limited resources. These are:

a) Short to intermediate term

- **Case acceptance criteria and prioritization criteria**—These criteria are important to decide: (1) what cases should be accepted and then (2) for those that have been accepted, what priority should be given to each case. Managers and section heads of Commercial Crime sections must allocate limited resources to incoming and ongoing investigations. The current resource allocation process is based on a subjective and largely initiative assessment of various factors, for example, type (seriousness) of the offence, value or size of the crime in dollar, age of the offence, availability of evidence, location of victims, etc. However, it is our understanding that no formal case screening criteria have been implemented and, certainly, not consistently across divisions.

  There must be a consistent and meaningful assessment of cases and their priority. This ensures that resources are allocated where needed and most effective and according to priorities. Additionally, applying the criteria provides an objective and visible basis for situations where a decision is made to not investigate a file. Formal case acceptance and prioritization criteria are being used in the Anti Racket's section of the Ontario Provincial Police. Exhibit VIII-5 provides examples of possible case acceptance criteria and possible prioritization criteria. A key criteria is that the case passes the National Interest Test (NIT) and falls within the mandate of the program. Once a complaint or case is received, the acceptance criteria should be immediately applied and the complainant or stakeholder informed about the decision. Cases that are accepted should then be prioritized against a rank system. Again, the complainant or stakeholder should be informed regarding the priority of the file. Files should be re-evaluated regularly against the prioritization criteria with an appropriate re-allocation of resources. The criteria and any prioritization weights should be developed at the national level with the input from the Sections. Once implemented, they should be communicated to stakeholders so they are aware of acceptance procedures for their files. At regular intervals (e.g., semi-annually, annually) NHQ Program management should monitor how the criteria have been applied and take any necessary corrective action. A decision-making and reporting tool can be used for applying criteria and recording/monitoring decisions.

- **Parameters for investigation timeframes and effort**—Setting these parameters can ensure that resources are used effectively. Investigations that have long durations run the risk of witnesses dying, evidence becoming stale and cases never being brought to trial. Particularly for large cases, there may have been a significant investment in resources and level of effort with no charges laid. Setting parameters, to the extent possible, can help reduce the risk of cases concluding without an outcome. If it is found that there are no charges to be laid or the complaint is unfounded, the resources can then be assigned to other priority cases. Other police organizations have indicated that they are setting maximum timeframes for investigations. For example, complex investigations projected to require 2,400 hours of investigation effort could be staffed by two investigators for one year instead of by one investigator for two years.

- **Teaming/partnering with other agencies**—Many of the stakeholders indicated that more teaming and partnering should be done. Teaming would allow the Program to build on skill sets and share intelligence or strategy.

Exhibit VIII-5
Potential case acceptance and prioritization criteria

Possible Case Acceptance Criteria	Possible Criteria for Prioritizing Accepted Cases
• National Interest Test (NIT) and whether federal or provincial. • Sufficient evidence to warrant a criminal investigation. • Better dealt with as a civil matter. • Facts investigated by another police service or regulatory agency. • All documentation necessary to prove the offence is in the file. • The complaint falls within the mandate.	• Public interest. • Offence likely to continue. • Availability/security of evidence. • Time required to investigate. • Value of the offence. • Location of victims. • Location of suspect. • Expected additional cost. • Likelihood of prosecution. • level of deterrence.

- **"Re-engineer" investigation requirements**—Various changes in how investigations are conducted could reduce resource requirements of individual investigations. The "savings" can then be reallocated to investigations with a resource deficit or to conducting more investigations. Some potential changes are:

  - Select/interview a smaller sample of victims in a group crime (50 vs. 200).

  - Establish guidelines/standards for submissions from complainants and, if standards are met, do not "re-do" the investigation. This may require providing advice to complainants while they prepare their submissions.

  - Advise on the appropriateness of civil remedies. In some cases, pursuing civil remedies may be more effective than criminal prosecution. This should be assessed when the file is received.

  - Establish the value of a fraud at a lower dollar level. If the value of a fraud, over a six month investigation, has been established at $750K, consider whether it is worth investing another three months of investigative effort to obtain the next $250K of fraud. The lower value may be sufficient for laying charges or bringing the case to trial.

  - Complainants/victims prepare their own statements. Corporate, regulatory or government complainants are likely capable of preparing their own statements and file documentation. They should be encouraged to do so according to guidelines set by the program.

  - Prepare electronic court briefs where Crown attorneys have the technology to accept them.

  - Locate closer to clients ("satellite" offices) on a temporary basis. Where sections are focused on particular areas, such as securities, investigative teams should be located nearby. This saves on travel time and costs, and facilitates informal sharing of information and communication.

- **Set national standards for the quality and completeness of evidence gathered by corporate, regulatory and government clients**—This benefits the stakeholder, as following the guidelines will facilitate their cases being accepted, for example, as according to the criteria in Exhibit VIII-5. Stakeholders may need to consult with Economic Crime investigators or management before investing too much effort in this to assess whether other case acceptance criteria may be met.

- **Minimize the learning curve by reducing the turnover rate of Economic Crime investigators**—Staff turnover results in handing off cases to other investigators or new staff. As a result, cases can take longer, lack continuity, or the investigations may not show results. Thus, reducing staff turnover contributes to the efficient and effective use of investigative resources.

- **Use project management disciplines and systems to establish milestones and track the progress of cases**—Other police organizations are employing project management tools and techniques to track the status of investigations. This includes assigning the cases to a responsible officer, setting up an expected timeframe for completion of the case, identifying key milestones and regularly and formally assessing the progress of the investigation against the milestones and expected timeframe. It is very important that team leaders or section heads review, at least weekly, the progress of cases being investigated by members of their team. Investigators may provide written or verbal status reports. Where progress is not according to plan, corrective action must be taken to get the investigation back on track.

- **Work more closely with stakeholders to discuss and assess cases**—As seen in some of the preceding observations, investigators may have to assume an advisory role for stakeholders. It has been suggested that investigators should work upfront with stakeholders to help them assess the merits of a case. This upfront investment of time is effective in managing the incoming caseload and, thus, the ongoing resource requirements.

- **Establish Service Level Agreements (SLAs) with internal support (e.g., informatics)**—There are concerns that, in some locations, the investigative teams are not getting the required level of support from the informatics units. As a result, technologically-inclined investigators are providing "super user" and "support desk" support for their colleagues. Also, there are concerns in some sites that the technology platforms available to Commercial Crime Sections are outdated. Negotiating and implementing SLAs between the in-house service providers (informatics, finance, staffing and other corporate management functions) and the Program itself, or specific locations of the Program, may help remedy this issue. The agreements foster and embed a customer service approach in support of the core work. They focus on service delivery quality within specified times and budgets. SLAs of this type have been implemented at the Serious Fraud Office (SFO) in the United Kingdom since April 1, 1997. SLAs must be reviewed regularly to be truly effective.

- **Improve MIS data integrity (quality assurance, up-to-date codes)**—MIS III is a key system for measuring operational performance. Since investigators each apply personal judgement in recording how their time spent on investigations is coded in the system, the consistency/accuracy of MIS data and, hence, the validity of the data in gauging performance, have been questioned. One concern is that it is difficult to get an accurate picture of the extent of tech crime where the computer is used as a tool in facilitating the crime. Survey codes have been set up but are not widely used. Greater attention to data integrity and quality assurance are needed. Good information is necessary for planning and monitoring resource usage.

b) Longer term strategies

- **Provide advice to government program developers on the implications of program design**—Economic Crime investigators could provide advice to government policy centres regarding the potential for criminal activity resulting from proposed programs. Good advice from the Economic Crime Program (ECP), and a willingness of program designers to incorporate their input, could allay some criminal activity. While this might require an upfront investment of resources by the ECP, it could reduce or contain the future caseload. At a minimum, the EC Program management would have some insight into potential areas of increased workload and could plan for it.

- **Hold more information seminars to raise awareness about scams and fraud**—Raising people's awareness about scams and frauds could reduce the number or magnitude of occurrences and, in turn, reduce incoming caseload.

- **Transfer minor investigations to other parties where police presence is not as critical and the risks of doing so are minimal, e.g., Student Loan fraud**—For example, the fully loaded cost of an Economic Crime investigation may exceed the cost to the Programs if this investigation were done externally.

- **Cost-recovery**—This is a longer term strategy for the Program that should be considered at the policy level. More and more federal departments are exploring this option. For example, the Department of Justice recently established three pilot cost-recovery projects (Canadian Heritage, Treasury Board Secretariat and Industry Canada). The two-year pilots will allow the Department and clients to assess the costs, benefits and feasibility of planning and delivering legal services on a cost-recovery basis. A cost-recovery regime might be suitable in the longer term for service on provincial contracts. Also, consideration could be given to charging back federal departments for investigations conducted on their behalf.

3. Ongoing resource management

The Program must have the appropriate infrastructure to manage resources on an on-going basis. Key areas are:

- **MIS III**. This operational system must provide accurate data and useful reports. Consideration should be given to adding a facility to estimate resource requirements for changes in workload volume.

- **Project management systems**. These systems should manage milestones, progress and resource loading. It is our understanding that, at present, there is not a system which records and monitors financial and salary costs of an investigation. This system should combine both so total costs can be monitored as the investigation progresses.

- **Activity-based costing systems**. These systems are useful to identify the costs of outputs and services to particular client groups and the associated overhead costs.

- **Performance reporting systems**. Program management must have appropriate performance reporting systems to monitor the quality of service delivery, throughput time, satisfaction, and cost. Outputs should be linked to program objectives to monitor performance against plan.

C. Training strategy and resources

Training is a critical resource for Economic Crime and Tech Crime investigators. However, there is no focus or strategy for Economic Crime training. Economic Crime investigators must receive frequent and, often specialized training to keep them up to date. Adequate training is essential for investigators to work as effectively as possible.

1. Training areas

- **Commercial Crime investigators** generally require the following basic training: a solid grounding and experience in investigation techniques including statement analysis and interviewing; basic accounting; business case law; understanding of computers and how to use them; and, business concepts. Those specializing in securities may require the Canadian Securities Market course (market groups). Investigators specializing in the mining or biotechnology industries may require courses in geology and chemistry, and biology, respectively. Some or all of this training could be obtained before they enter the program.

- With the proliferation of technology, traditional areas for evidence are changing. Appointment books and Rolodexes are being replaced by pocket organizers and electronic calendars on computers. **Field investigators** within and outside of Economic Crime need to be aware of new sources for evidence for crimes and how to protect potential evidence (e.g., turning on a computer could destroy dates and times on the hard drive which would otherwise support/refute a suspect's alibi).

- **Tech crime investigators** must be more than literate with computers. Actual training requirements would depend on the investigator's level of knowledge. However, these must be kept current. One division's training request for tech crime investigators included networking essentials, Digital basic and advanced for Unix boxes and the Internet, supporting and administration for MS95, supporting WinNT, supporting WinNT enterprise, intranetware, netware advanced administration, advanced Internet security, Interneting with TCPIP protocol, and electronic sources of information. Costs for this training were estimated at roughly $22,000 per investigator.

- **Technical operations investigators** require advanced training and it has been suggested that officers identified in this capacity return bi-annually to learn about the newest forensic techniques for technology. It was suggested that an initial certification be required with regular re-certification. This would assure the qualification of the investigator as an expert witness and as a certified examiner, thus avoiding challenge and the resultant development of bad case law. Areas of expertise in the RCMP with training and certification requirements (from 6 to 13 weeks) are polygraph, Ident and bomb technicians. However, tech crime does not currently have such a requirement. Besides having a very strong computer and Internet background and years of experience in the computer area including programming, systems and hardware, and investigative experience, these investigators could obtain training in the computer forensics course from the Canadian Police College, and take courses from various providers which we understand to be the International Association of Computer Investigation Specialists, the Federal Law Enforcement Training Centre (FLETC), Coordinated Law Enforcement Unit (CLUE) and the National Consortium for Justice Information and Statistics (SEARCH) which offers computer forensics training.

2. Training options

Currently, there is no entitled training or a training standard (for entering the program or learning while on the program) for Tech Crime investigators. These members must take their own initiatives to find appropriate tech crime training from externally available courses (such as university or technical college courses, Internet courses from Learnquest, Novell Administrator certification) or from among the options available within the RCMP.

There is a need for Commercial Crime core training with specialized knowledge—the latter often provided by partners. Commercial Crime investigators are obtaining training from a variety of sources: municipal police departments, provincial forces, individual sections, regulatory bodies (e.g., securities commissions, stock exchanges), universities, accounting firms, and bankruptcy trustees. The Commercial Crime investigators course, as it currently stands, is perceived to be primarily suitable for candidates seeking to enter Commercial Crime, or who have recently entered the Program.

There are three types of training available through the RCMP for Economic Crime investigators:

- **Centralized:** "Force-wide" training, basically, a "national standards" type of training whereby participants across the country would receive the same training to meet the needs of the force. Trainers travel to the training site and deliver a standard course. Funds for centralized training are allocated according to the department's national priorities. In the past, a Commercial Crime Investigators Course was offered. Its purpose was to prepare newly employed Commercial Crime investigators for their operational duties. The material on the course was recognized as primarily at the introductory level to give all candidates the ability to investigate frauds and related offences including knowledge of law, search warrants, interviewing, and handling evidence. It also familiarizes them with various enforcement areas which are the responsibility of the Economic Crime Directorate including offences involving the Income Tax Act, commercial organizations, accounting procedures, stock markets and securities. The course also covered bankruptcy offences, stock market manipulations, effective interviewing, and development and retention of sources of information.

  One component of the course introduced the participants with some of the common offences when dealing with computers and the investigative procedures to be followed prior to, during, and after a search of a computerized office. Exhibit VIII-6 presents the general topics covered in the Computer Crime session. It appears that the course has not been amended since 1992 and is deemed to be not representative of what is required in this area today. In 1997/98, the course was not run as there were concerns that it had to be revised and that funds were returned to the HQ Programs. In the technical operations area, we understand that a course has not been offered in the last four years and that a course in this area did not make the priorities list and would be considered duplicative of that offered by the Canadian Police College.

  It is our understanding that the Commercial Crime course is under review to bring it in line with new decision-making models in the Department and the employee continuous learning approach. Also, an initiative is underway to define core competencies for Commercial Crime investigators. This is an input to a learning strategy for these investigators.

- **Divisional:** This is similar to centralized training but it is specific to a province such as a course that has to be modified for geographic concerns. It does not appear to have been used widely for Commercial

Crime investigators. The officers we spoke with were not aware of any formal divisional training with a tech crime focus. We were advised that significant research and development is required to prepare a tech crime course and the tech crime communities within the divisions are too small to warrant the investment. Additionally, there is an investment required in keeping the course up-to-date because technology is changing rapidly.

- **Canadian Police College (CPC):** The CPC provides training for law enforcement entities across Canada. It is generally relied upon as the standard in the computer forensic area, and is likely the only provider of a tech crime forensic computer course. It offers training in "Computer Crime Investigative Techniques". The curriculum of four courses includes: Electronic Search and Seizure (a two-week course offered roughly 5-6 times per year on how to seize and search standalone DOS computers; Network Principles and Investigative Techniques (a two-week course offered three times per year providing an introduction to Novell and NT (MS) LANs and circumvention of security; Telecommunications Fraud and Investigative Techniques (a two-week course offered twice a year which addresses telephone technology, Internet access and searching the Internet); Electronic Search and Seizure for the Macintosh" (a two-week course offered once per year on how to search and seize standalone Macintosh computers.

It was noted that most officers working on tech crime investigations regularly have been trained. Under the current regime, the RCMP is competing with other police forces for seats in their training program. Training requests are forwarded from Divisions and police forces to the CPC which then allocates seats based on the size of the force. The CPC provides training based on demand and available CPC resources. It is estimated that 50% of the demand is met. It is our understanding that the CPC is discussing a cost-recovery regime. A rough benchmark for potential tuition costs under cost-recovery would be $1,000 per two-weeks.

Exhibit VIII-6
Current Commercial Crime Investigators Course: Computer Crime Topics

- Definition of:
  - Computer.
  - Computer systems.
  - Computer programs.

- Incidence of computer crime:
  - Research estimates.
  - Numbers/types of investigations.

- Laws pertaining to computer crime:
  - Criminal code.

- Computer Services:
  - Section 342.1 C.C. - Illegal Access.

- Section 430 (1.1) C.C. - Mischief.

- Software and Confidential Information:
  - Section 322 C.C. - Theft.
  - Section 380 C.C. - Fraud.

- Section 354 C.C. - Possession of Property Obtained by Crime:
  - Section 357 C.C. - Bringing into Canada.
  - Section 358 C.C. - Possession.
  - Section 406 C.C. - Forging Trademark.
  - Section 411 C.C. - Defacing, Concealing, or removing Trademark.
  - Section 412 C.C.-Punishment for Trademark Violations.

- Copyright Act:
  - Section 2 - Definition Computer Program.
  - Section 12(3) - employer ownership.
  - Section 17(2)(1) - copying.
  - Section 17(2)(m) - copying.

- Infringements:
  - Section 42 - sale.
  - Punishment.
  - Patents Act (as it pertains to computers).

Exhibit VIII-6 (cont'd)
Current Commercial Crime Investigators Course: Computer Crime Topics

Problems encountered investigating computer related crime:

- Complexity.
- Difficulty.
- Cost.
- Easy destruction.
- Legal problems.
- Inexperience.

Differences between computer assisted crime and traditional white collar crime:

- Forms of assets.
- Occupations of perpetrators.
- Environments.
- Modus operandi.

Classes of threats to EDP assets:

- Destruction.
- Removal or loss.
- Corruption or modification.

Resources:

- Security officers.
- Specialists.
- University resources.
- Manufacturer.
- City police.
- Provincial police.
- RCMP.

Search warrant:

- Computer program.
- Computer system.
- Data.
- Computer service.
- Function.

Search team:

- Meeting.
- Designation.

Equipment:

- Needs for search and exhibits.

Solicitor client privilege:

- Section 488.1(2) C.C.
- Section 488.1(3) C.C.
- Section 488.1(4) C.C.
- Section 488.1(6) C.C.
- Section 488.1(8) C.C.

Auditing:

- Without a computer.
- With a computer program.
- With a computer.

Exhibit VIII-6 (cont'd)
Current Commercial Crime Investigators Course: Computer Crime Topics

At the end of this session, each candidate will be able to correctly and without the use of references:

1. Define a computer, computer system and computer program.
2. Identify the appropriate sections of the criminal code for:
   - Illegal/access.
   - Mischief.
   - Theft.
   - Fraud.
   - Illegal possession.
3. Identify the appropriate sections of the copyright act for:
   - Employer ownership.
   - Illegal copying of program.
4. List six problems encountered when investigating computer related crime.
5. List six investigative steps to be undertaken before conducting a search

Source: Commercial Crime Investigators Course, Course Training Standard, June 1992.

Tech Crime courses must be updated regularly due to the rapid pace of technological change. A potential training strategy for Tech Crime which has not yet been formally explored is to "piggy-back" on the investments that other organizations have made and thus save the up-front development costs. Two examples are:

- **Canadian Police Research Centre (CPRC):** The RCMP, the National Research Council (NRC) and the Canadian Association of Chiefs of Police (CACP) are partners in the CPRC. Its mission is to provide leadership and focus for a national program of R&D, evaluation and commercialization in the law enforcement and public safety sectors in Canada. It has as its objectives to see that the best equipment possible is available to Canadian Police agencies and to offer Canadian enterprise an opportunity to develop a capability in this specialized market. A couple of years ago, the CPRC started to get involved in matters relating to computers. It started by setting up list servers on the Internet, including one on high tech crime which allows computer forensic investigators from accredited law enforcement agencies to post newsworthy items such as what is considered acceptable evidence. It also set up a password protected web board which posted handouts from the Canadian Police College.

The CPRC is now venturing into training. It is now developing and testing an investigational techniques course for the Internet which will be delivered to course candidates over the Internet. It is currently designed for the general duty investigator and will cover Internet search capabilities and open source information available on the Internet. This course can be offered at a substantial saving over the cost of centralized training. The costs for developing and delivering this course are $3,400. The CPRC is planning to offer a course on encryption over the Internet.

- **Infotech Training Working Group, U.S. Department of Justice:** The CPRC, through its Public Safety Network[16] is working with the Computer Crime and Intellectual property Section of the U.S. Department of Justice, through their Infotech Training Working Group, to "fast-track" the development of six training courses for computer crime investigators and trainers. The courses under development are a video on the basics of computer investigation, CyberCop 101, CyberCop 201, Advanced Internet Investigations, Network Intrusions, and a Train the Trainers course. These courses will be shared with interested law enforcement agencies for free. Thus, these courses could be delivered within the RCMP for a minimal start up cost of organizing for the training and making small adjustments for Canadian relevance. Updates are provided free as well, thus ensuring that the course is state of the art. This initiative has been agreed to by both the Commissioner of the RCMP and the Attorney General of the United States. It is our understanding that this option is being pursued and a working group has been set up.

Clearly, there are various options available for providing training to Economic Crime and Tech Crime investigators. These are:

- Centralized training.
- Divisional training.
- Canadian Police College training.

---

[16] *The PSN partners are: Canadian Association of Chiefs of Police (CACP); Canadian Police College (CPC); Canadian Police Research Centre (CPRC); COPNET; Edmonton Police; Canadian Institute for Scientific and Technical Information (CISTI) of the National Research Council.*

- Internet-based training as through the CPRC.
- Infotech Training Work Group training.
- External/private sector training.
- On the job training (e.g., understudy program).
- A combination of training methods.

The Program should control and allocate training funds. It is extremely important that the Economic Crime Program identifies and formalizes the training requirements and standards for Commercial Crime investigators, Tech Crime investigators and those interested in joining the program. This is a key input to identifying and recommending/selecting training options. Program management must also decide whether a certification and re-certification program is required for Tech Crime investigators. Another consideration is whether basic "pack it and bag it" training (and regular re-freshers) on procedures for protecting evidence from computers and technology should be provided to investigators outside of tech crime. Other basic training would include electronic search and seizure for appropriate search techniques for technology and where data can be found (vs. intimate knowledge about hard drives).

Core training must be provided consistently with a variety of options for specialized knowledge (e.g., partnering). The training options should be assessed against criteria which supports the training strategy. Exhibit VIII-7 assesses tech crime training options against some potential criteria. As can be seen, there are trade-offs between the options. For example, while centralized training is highly consistent (in that all participants force-wide receive the same training), the R&D, delivery and update costs are significant for the Department. On the other hand, tech crime training offered through the Infotech Working Group would have no or minimal R&D, delivery and update costs, yet the training courses are not yet recognized as a "standard". The rapid pace of change of tech crime courses must be taken into account when selecting/funding training providers. Short development periods are preferable so that material is current. Once these decisions are made, the Program should select and negotiate with the various training providers).

D. Technology resources

Technology is a critical resource for Tech Crime investigators in particular, but Economic/Commercial Crime investigators also need the required technology to work productively and effectively. Tech support investigators need to have the technology to enhance the productivity and capability of the investigative services and support provided. They need the ability to search, seize and analyze hardware, software and evidentiary data. Laptops and Jaz drives enhance their ability to assist or analyze at search sites. Project rooms or labs should have the capability to back up large volumes of important and sensitive evidentiary data to suitable media for the commercial crime or tech crime investigators. Since commercial crime and tech crime investigators in the field are often on the road, each would benefit from having a laptop computer and a cellular phone.

Technology is also an extremely expensive resource. To ensure that it is being used effectively where required by the program, NHQ Program Management should allocate and control technology funds. We are not aware of a "standard" configuration that has been established for Economic/Commercial Crime investigators. It is very important for Program Management to decide on the technology standards, equip members to a standard and provide the annual for storage media and workstation upgrades processing speed and capacity. Exhibit VIII-8 shows the basic technology requirements for Tech Labs, tech crime investigators and commercial crime investigators. They have been compiled from interviews.

Set up costs for a tech lab configuration (four-workstation lab) as shown are about $100,000 (exclusive of accommodations). Annual upgrades are estimated at $20,000 for workstations and new technology as it comes to market. HTF in the Tech Ops Directorate has just acquired this equipment to get to the state of the art. The equipment depicted would be a basic requirement in regional tech labs, though the set up and maintenance costs may be less if there are fewer workstations required. At present, there are high tech crime forensics labs, of varying size and scope, in Montreal, Vancouver, London and Edmonton. Vancouver, in particular, identified a requirement for new equipment to upgrade the technology of the tech support and Commercial Crime investigators of $191,400 for various equipment to support an establishment of some 60 members. A rough cost for fit up for investigators might be $10,000 per capita with annual maintenance of $5,000 for new technology in laptops, workstations and storage media.

NHQ Program Management provided each division with an "equipment kit" for a laptop and a Jaz drive ($6,500 each from special initiatives funding) to download information for forensic purposes without seizing the computer. The equipment was provided to the division Commercial Crime sections for the Tech Crime investigators. NHQ also provided about $200,000 for the purchase of hardware and software to enhance the forensic capability at divisional sites.

It is difficult to predict with any certainty the future technological requirements since technology is changing so rapidly. However, it is expected that investments will be required in larger storage media (which is always increasing) and the processing speed of workstations. Larger storage media is necessary for searches where speed is important for the investigators to back up the data. Labs may also require Vogon, a forensics software package from the United Kingdom which enables drive imaging and analysis.

Exhibit VIII-7
Comparison of Tech Crime training options

	Centralized	Divisional	CPC	CPRC	Infotech Working Group	Private Sector/ Universities, etc.
Consistency	• All participants force-wide receive same training	• All participants in a division, province, region receive same training with a local flavour	• The "standard" across jurisdictions in the computer forensic area	• Same content is available to all course candidates through the Internet, assuming they follow the curriculum	• Not an official "standard", but training is of interest to Canadian and US law enforcement agencies	• No consistency among externally available courses. • Depends on investigators' level of knowledge
R&D Cost	• Significant for RCMP plus, multi-year timeframe for development	• Significant for RCMP • Tech Crime communities in the divisions too small to warrant the investment	• Significant for CPC plus multi-year, timeframe for development	• Minimal for CPRC	• Courses to be shared with law enforcement agencies for free	• No cost to RCMP
Delivery Cost	• Significant	• Significant	• Potential tuition costs ($1000/2 weeks) under cost recovery	• Minimal for CPRC • Minimal costs to RCMP to access courses	• For RCMP, minimal start up cost for organizing the training and making Canadian customization	• Tuition costs for a variety of courses
Update Costs	• Significant	• Significant	• Significant for CPC	• Minimal for CPRC	• Updates provided free to RCMP • Some customization by RCMP required	• No cost to update for RCMP, but update courses require tuition fee
Accessibility	• Course training requirement must make the priorities list • Training need must be approved for	• Training need must be approved for candidate	• RCMP is competing with other police forces for seats	• Available to investigators with an Internet account	• Could be made available to all who require if delivered internally	• Investigators must take own initiative to find/attend course • Courses may not be as widely accessible depending on location of course

Exhibit VIII-8

Potential equipment requirements for Economic Crime and Tech Crime

	Tech Labs (high tech crime forensic)	Tech Crime Investigator	Commercial / Economic Crime Investigators
Hardware			
• Workbenches	√		
• Full tower workstation with a SCSI card	√	√	
• State of the art workstation (e.g., Pentium) with large size hard drive			√
• Network card	√	√	√
• Multiple hard drives (with large volume capacity)	√	√	
• Rewritable CD-ROMs, external type to portable	√	√	
• CD-ROM reader-writer	√	√	
• Portable/removable storage media:			
– iomega Jaz hard drive	√	√	√
– iomega Zip drive	√	√	√
• Exabyte tape drive, 4 milimeter	√	√	
• Good quality monitor (colour)	√	√	√
• Notebook computers (SCSI card, Pentium, modem for Internet)	√	√	√
• High speed laser jet printer	√	√	
• Laser jet printer (good quality)			√
Software			
• Norton Utilities	√	√	√
• Partition Magic	√	√	
• RCMP investigative utilities	√	√	
• Safeback (imaging program)	√	√	
• Drive imaging and analysis	√	√	
• Supergravity/Supertext	√	√	
• Internet account/access	√	√	√
• Commercially available office suite with wordprocessing, spreadsheets, e-mail, etc.	√	√	√
Telecommunications			
• Cellular phone	√	√	√
• Cellular phone account	√	√	√
Other			
• Private office			√
• Lab space/lockers	√	√	
• Vehicles		√	√

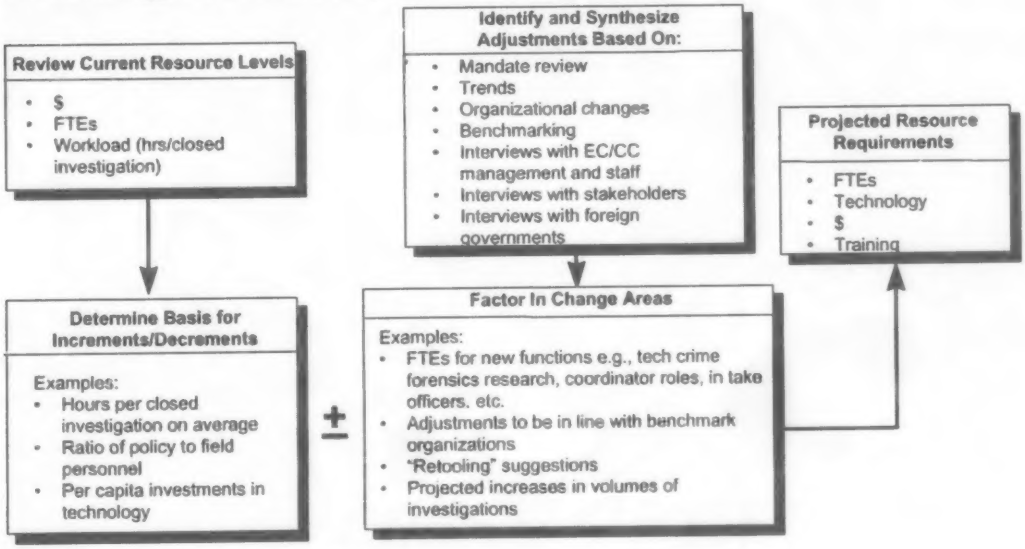
These are not final requirements and they will vary by site. However, they should be discussed by management within the Economic Crime Program, Informatics, the Tech Ops Directorate, and the Divisions to obtain consensus on the requirements, develop standard configurations, and develop a strategy for acquiring the items as these will be substantial technological investments.

It is our understanding that sites are at varying levels of sophistication of the technology for the labs and the investigators. Ideally, equipment requirements should be set so that each division has the same baseline technological capability. Then, where there are special/unique circumstances, or where volume warrants it, additional equipment should be provided.

E. Resource requirements

This section describes our methodology for determining the Program's resource requirements and presents our estimates. Exhibit VIII-9 depicts our approach for determining the requirements.

Exhibit VIII-9
Methodology for determining resource requirements



Review Current Resource Levels
$
FTEs
Workload (hrs/closed investigation)
Identify and Synthesize Adjustments Based On:
Mandate review
Trends
Organizational changes
Benchmarking
Interviews with EC/CC management and staff
Interviews with stakeholders
Interviews with foreign governments
Projected Resource Requirements
FTEs
Technology
$
Training
Determine Basis for Increments/Decrements
Examples:
Hours per closed investigation on average
Ratio of policy to field personnel
Per capita investments in technology
±
Factor In Change Areas
Examples:
FTEs for new functions e.g., tech crime forensics research, coordinator roles, in take officers, etc.
Adjustments to be in line with benchmark organizations
"Retooling" suggestions
Projected increases in volumes of investigations

1. Resource allocations in other police organizations

As input to estimating the resources for the Economic Crime Program, we sought information on resource allocations from other police organizations. We asked for: information on FTEs and budgets (to the extent possible by type of crime and Headquarters vs. field); information on trends and future growth areas; and benchmarking information such as new cases, cleared/closed cases and level of effort.

We made contact with the following organizations:

- Serious Fraud Office (SFO).
- Australian Federal Police (AFP).
- Federal Bureau of Investigation (FBI).
- Metropolitan Toronto Police Fraud Squad.
- Ontario Provincial Police.

We approached New Scotland Yard but we were unsuccessful in getting information on interviews as the contact was unavailable during the required timeframe. We also spoke with the Office of Strategic Assessment of Australia, primarily a policy centre.

We did obtain resource allocation information, though to various degrees from each organization. Unfortunately, this information cannot be used for a direct comparison of resource allocations because of differences in mandates, the basis on which the statistics are compiled, the definitions of offences, the reporting of information, organizational structure, and definitions of input and output. However, the information does illustrate some patterns. A key common theme is that these organizations are taking steps to manage their resources and monitor resource consumption.

The relevant information we were able to obtain from each is discussed below:

a) Serious Fraud Office (SFO)

The aim of the Serious Fraud Office (SFO) is "to investigate and prosecute serious and complex fraud and so deter fraud and maintain confidence in the probity of business and financial services in the United Kingdom".[17] The

---

[17] *Serious Fraud Office, Annual Report 1996-97.*

Office investigates cases referred from police, the Department of Trade and Industry, the Crown Prosecution Service, Self Regulatory Organizations, the Bank of England, the SFO itself and other sources. Exhibit VIII-10 shows the trend in the expenditures and staff since 1989. Overall, total expenditures have increased, but are at their lowest level since 1990/91. Total staff have increased since 1992/93 by 3%. A small rise in the number of permanent staff in 1996/97 reflects the SFO's policy of building up financial investigative expertise within the SFO. They indicate that this reduces expenditures on accountants from private sector firms and makes it possible for the office to investigate the increased number of cases within existing resources. It also ensures that experience remains within the Office.

Exhibit VIII-10
United Kingdom—Serious Fraud Office: expenditures (£ in millions) and staff

	1989/90	1990/91	1991/92	1992/93	1993/94	1994/95	1995/96	1996/97 Provision	1997/98 Budget
Administration	5.76	6.62	8.95	10.16	10.88	10.84	10.71	10.4	9.76
Investigations and Prosecutions	3.45	6.57	8.76	10.87	8.15	7.19	6.62	6.59	6.16
Total Expenditures	**9.21**	**13.19**	**17.71**	**21.03**	**19.03**	**18.03**	**17.33**	**16.99**	**15.92**
Permanent	-	-	117	136	138	137	162	166	-
Temporary	-	-	-	67	57	52	43	44	-
Total Staff	**-**	**-**	**-**	**203**	**195**	**189**	**205***	**210**	**-**

Source: Serious Fraud Office Annual Reports, 1992/93 through 1996/97.

Includes 38 financial investigators. Twelve new permanent positions were created. In 1994/95, there were 31 accountants and investigators

Since 1992/93, the length of time between case acceptance and transfer for prosecution has increased from 15 months to 19.2 months. The trend is depicted in Exhibit VIII-11. During this period, evidence must be obtained from overseas and this is taking longer. Detailed accounting analyses also take time.

Office investigates cases referred from police, the Department of Trade and Industry, the Crown Prosecution Service, Self Regulatory Organizations, the Bank of England, the SFO itself and other sources. Exhibit VIII-10 shows the trend in the expenditures and staff since 1989. Overall, total expenditures have increased, but are at their lowest level since 1990/91. Total staff have increased since 1992/93 by 3%. A small rise in the number of permanent staff in 1996/97 reflects the SFO's policy of building up financial investigative expertise within the SFO. They indicate that this reduces expenditures on accountants from private sector firms and makes it possible for the office to investigate the increased number of cases within existing resources. It also ensures that experience remains within the Office.

Exhibit VIII-10

United Kingdom—Serious Fraud Office: expenditures (£ in millions) and staff

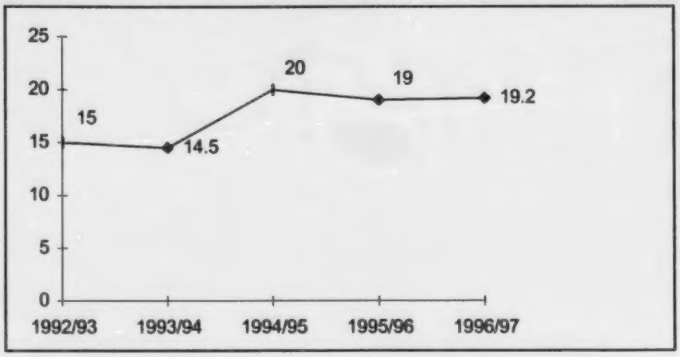
	1989/90	1990/91	1991/92	1992/93	1993/94	1994/95	1995/96	1996/97 Provision	1997/98 Budget
Administration	5.76	6.62	8.95	10.16	10.88	10.84	10.71	10.4	9.76
Investigations and Prosecutions	3.45	6.57	8.76	10.87	8.15	7.19	6.62	6.59	6.16
Total Expenditures	**9.21**	**13.19**	**17.71**	**21.03**	**19.03**	**18.03**	**17.33**	**16.99**	**15.92**
Permanent	-	-	117	136	138	137	162	166	-
Temporary	-	-	-	67	57	52	43	44	-
Total Staff	**-**	**-**	**-**	**203**	**195**	**189**	**205***	**210**	**-**

Source: Serious Fraud Office Annual Reports, 1992/93 through 1996/97.

Includes 38 financial investigators. Twelve new permanent positions were created. In 1994/95, there were 31 accountants and investigators

Since 1992/93, the length of time between case acceptance and transfer for prosecution has increased from 15 months to 19.2 months. The trend is depicted in Exhibit VIII-11. During this period, evidence must be obtained from overseas and this is taking longer. Detailed accounting analyses also take time.

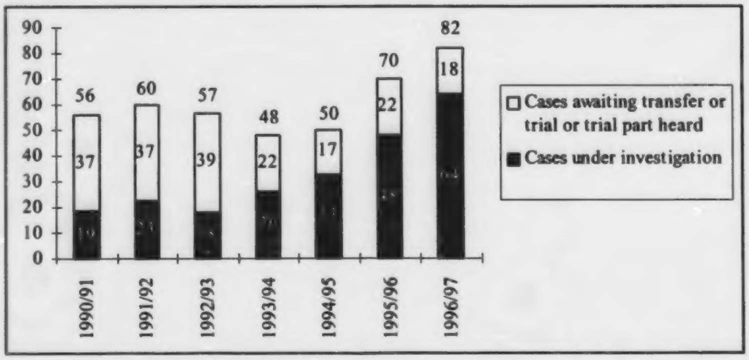
Exhibit VIII-11
United Kingdom—Serious Fraud Office (SFO), length of time between case acceptance and transfer to the Crown court or committed for trial



Source: Serious Fraud Office, Annual Reports 1992/93 through 1996/97.

Exhibit VIII-12 shows the trend in total active caseload for the SFO between 1990/91 and 1996/97. There has been a dramatic increase in the volume of total caseload (46%), and especially an increase in the volume of cases under investigation (236%). Part of the increase in caseload is attributable to changes implemented in 1995 in the criteria for acceptance of a case including the lowering of the financial threshold to £1 million.

Exhibit VIII-12
United Kingdom—Serious Fraud Office (SFO), Total Active Caseload 1990/91 through 1996/97



Source: Serious Fraud Office, Annual Reports 1992/93 through 1996/97.

(Cases represented in SFO statistics are all higher than £2 million).

Note: Criteria for acceptance of a case were changed and the financial threshold lowered in March 1995. This accounts for the 64% increase in current caseload since 1994/95.

Since 1992/93 [the first year for which we have volume and expenditure information (as per Exhibit III-10) available], the ratio of expenditures per case under investigation has dropped by 77% from £1.168 million to £.266 million. We do not know the precise reasons for this, though the documentation discusses:

- A reorganization of the office into a number of multi-discipline divisions staffed by lawyers, accountants and law clerks. This simplifies management control and allows the operational staff to be more closely aligned on each case.

- A commitment to keeping the investigation of cases as short as possible, balancing that against the need to conduct a thorough and effective investigation. Realistic targets are set for each case, and progress is measured against those targets on a monthly basis.

- Delegation of budgets for investigations and prosecutions to division heads so that those incurring expenditures hold budget responsibilities. Those responsible for managing cases are held accountable for management of their costs. Delegated budgets are monitored centrally and each assistant director is obliged to justify each element of the budget.

- Establishment of a policy division responsible for all policy and procedural issues with a bearing on the SFO's work. It addresses non-operational activities such as the vetting of cases, liaison with outside bodies and changes to legislation. These activities had previously been handled by individuals in addition to their main caseload.

- Continuing reviews of how support services are provided to ensure that they more effectively benefit the investigation and prosecution of cases. This includes:

    - Improvements to case planning systems.

    - Widening of the role of support staffs to assist financial investigators as well as lawyers.

    - Establishment of SLAs between the in-house service providers and the integrated divisions.

- A new finance system which meets the Office's need for individual case accounting, facilitates the introduction of resource accounting and budgeting, and improves payment performance.

- Increases in permanent staff and a decrease in the expenditures on external accounting firms. This makes it possible to investigate the increased caseload within existing resources and ensures that experience remains within the Office.

- On-going training of staff in different areas including a residential project management course.

Exhibit VIII-13 indicates trends in the types of fraud investigated by the Office. Frauds on banks and financial institutions is the predominant type of fraud in 1996/97. Caseload in this area has more than doubled since 1993/94.

Exhibit VIII-13
United Kingdom—SFO, Types of Fraud involved in SFO caseload

Types of Fraud	1993-94	1994-95	1995-96	1996-97
Fraud on banks/financial inst.	20	14	29	42
Fraud on creditors	25	21	18	17
Fraud on investors	11	21	16	17
Fraud on central/local government	4	5	8	10
Fraud involving manipulation of financial markets	9	4	3	3
Others	10	7	16	14

Source: Serious Fraud Office Annual Reports: 1993-1997.

b) Australian Federal Police (AFP)

The AFP is viewed by the Australian government as a prime instrument of federal law enforcement. Its role is to preserve the integrity of the Commonwealth Criminal law and interests as they are threatened by criminal activity within Australia and beyond its shores. The AFP's core business priorities include:

- Investigation of the more serious levels of fraud against the Commonwealth.

- Investigation of major organized crime.

- International drug trafficking.

- Undertaking special referrals from the federal government.

It also meets obligations under the Commonwealth Fraud Control Policy.

We understand that it has recently been refining the focus of the business it does and rationalizing the extent of work it performs. For example:

- The AFP will only undertake the large and/or complex operations which impact the structure of criminal enterprises. Small, less complex investigations are the responsibility of federal departments and agencies. However, the AFP provides training and support to these organizations as required.

- In order to ensure a consistent national approach to evaluating and prioritizing of factors, the National Assessment and Prioritization (NAP) model, in determining the priority to be allocated to all referrals and tasks requiring the commitment of resources.

Exhibit VIII-14 shows the trends in operating budgets and staff of the AFP for 1990/91 through 1997/98. Overall, the operating budget has increased by 12% while the total staff has declined by 18%. There has been an overall decrease in the number of police members of 20% and an increase in the number of staff of 3.3% between 1990/91 and 1996/97. Not all police members conduct investigations—some are employed in personnel management, training, legal, liaison, criminal records and policy. Some staff members are employed in areas such as intelligence and telephone interception. Information was not available at the program level.

Exhibit VIII-14
Australian Federal Police—Trends in operating budgets and staff

		STAFF		
Year	**Budget $M (AUS)**	**Police Members**	**Staff**	**Total**
1990-91	220.0	2,543	674	3,217
1991-92	229.6	2,453	701	3,154
1992-93	226.4	2,394	666	3,060
1993-94	244.8	2,302	740	3,042
1994-95	257.1	2,284	724	3,008
1995-96	272.4	2,117	690	2,807
1996-97	258.0	2,027	696	2,723
1997-98	246.0	-	-	2,624

Source: AFP.

We were informed that current AFP financial and staffing systems do not allow the identification of resources devoted to specific categories of investigations such as economic crime. We were able to obtain some information on expenditures for investigation areas that appear to correlate with areas under the Economic Crime Program. Exhibit VIII-15 depicts the 1997/97 actual and 1998/99 budgeted expenditures for investigations in the areas of "economic crime" and "corruption". Expenditures for investigations are anticipated to decrease by almost 5%. Overall AFP expenditures, on the other hand, are expected to have only a minimal decrease. We have no information on the FTEs corresponding to these investigation areas.

Exhibit VIII-15
Australian Federal Police—1997/98 (Actual) and 1998/99 (Budgeted) expenditures for criminal deterrence

Output	Expenditures ($000s Aus)	
	Actual 1997/98	**Budgeted 1998-1999**
Economic Crime*	$30,679	$29,279
Corruption**	$3,710	$3,499
Sub-Total	**$34,389**	**$32,778**
External Agency Support***	$22,820	$213,074
AFP Total Expenditures for criminal deterrence******	**$132,884**	**$132,089**

Source: AFP

* *Economic crime includes investigations of fraud, corporate crime, money laundering and other economic crime (intellectual property, bankruptcy, computer crime/telecommunications, counterfeiting and environmental crime.*

** *Corruption includes investigations of administration of justice, electoral, bribery, and disclosure of information.*

*** *Reflects the AFP's partnerships through joint investigations and liaison programs with other agencies and providing training for them in some cases.*

**** *"Criminal deterrence" is considered an "outcome area 1". We do not have a complete list of other outcome areas. This would account for the discrepancy between the budget figures in Exhibit VIII-14 and the total expenditures in this exhibit.*

We were informed that current AFP financial and staffing systems do not allow the identification of resources devoted to specific categories of investigations such as economic crime. We were able to obtain some information on expenditures for investigation areas that appear to correlate with areas under the Economic Crime Program. Exhibit VIII-15 depicts the 1997/97 actual and 1998/99 budgeted expenditures for investigations in the areas of "economic crime" and "corruption". Expenditures for investigations are anticipated to decrease by almost 5%. Overall AFP expenditures, on the other hand, are expected to have only a minimal decrease. We have no information on the FTEs corresponding to these investigation areas.

Exhibit VIII-15
Australian Federal Police—1997/98 (Actual) and 1998/99 (Budgeted) expenditures for criminal deterrence

Output	Expenditures ($000s Aus)	
	Actual 1997/98	**Budgeted 1998-1999**
Economic Crime*	$30,679	$29,279
Corruption**	$3,710	$3,499
Sub-Total	$34,389	$32,778
External Agency Support***	$22,820	$213,074
AFP Total Expenditures for criminal deterrence****	**$132,884**	**$132,089**

Source: AFP

* *Economic crime includes investigations of fraud, corporate crime, money laundering and other economic crime (intellectual property, bankruptcy, computer crime/telecommunications, counterfeiting and environmental crime.*

** *Corruption includes investigations of administration of justice, electoral, bribery, and disclosure of information.*

*** *Reflects the AFP's partnerships through joint investigations and liaison programs with other agencies and providing training for them in some cases.*

**** *"Criminal deterrence" is considered an "outcome area 1". We do not have a complete list of other outcome areas. This would account for the discrepancy between the budget figures in Exhibit VIII-14 and the total expenditures in this exhibit.*

fs

Exhibit VIII-16 shows the trends in workload and cases by type of offence corresponding generally to the Economic Crime Program types. Information on the level of effort devoted to these specific offences could not be provided. The exhibits indicate that:

- Fraud referrals to the AFP have been declining since 1992/93. We understand that, in accordance with Australian federal government policy, Commonwealth agencies have been increasingly undertaking minor fraud investigations themselves. We were also informed that there are indications that Commonwealth agencies may be increasingly turning to private sector providers for fraud investigations.
- The AFP is drastically reducing its backlog (which we interpret to be "Matters on Hand") of fraud cases (from 2,882 in 1992/93 to 315 in 1996/97), likely due to the decrease in referrals. In 1996/97, for every case initiated, there was just over one completed. This is a decrease in the completion rate compared to the rate set in previous years.
- The volume of bankruptcy investigation referrals has declined since 1992/93. The ratio of completed to initiated cases has been declining since 1994/95.
- The volume of computer crime investigation referrals has increased by 46% since 1992/93. The volume grew 76% in 1996/97 over 1995/96 and 1994/95 levels.
- Referrals of counterfeit currency investigations have fluctuated since 1994/95. Overall, the volume has decreased by 37%.

Exhibit VIII-16
Australian Federal Police—Trends in cases and workload by type of crime

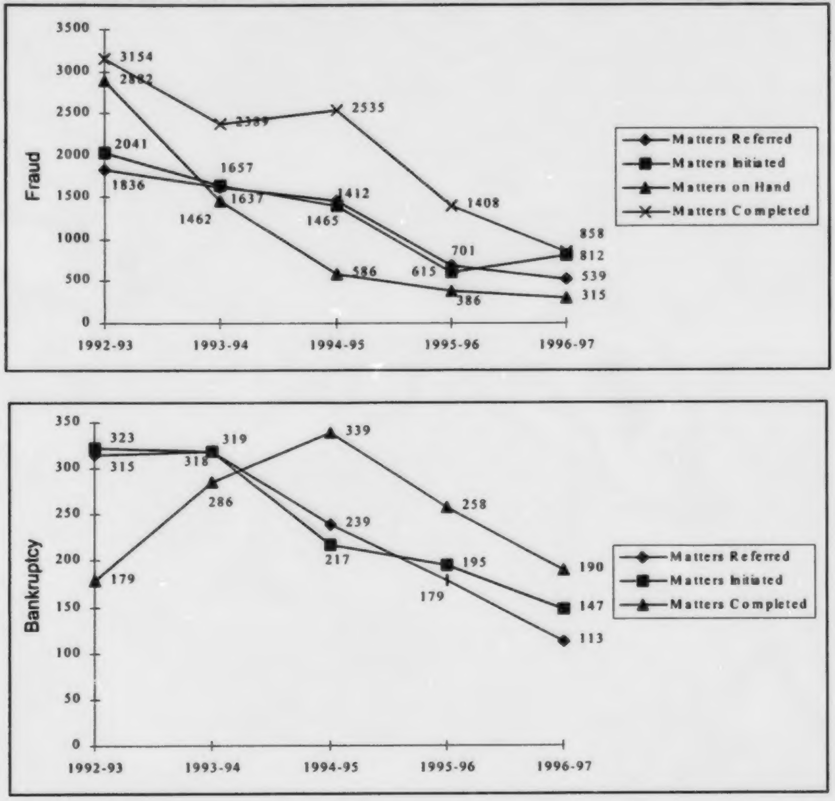
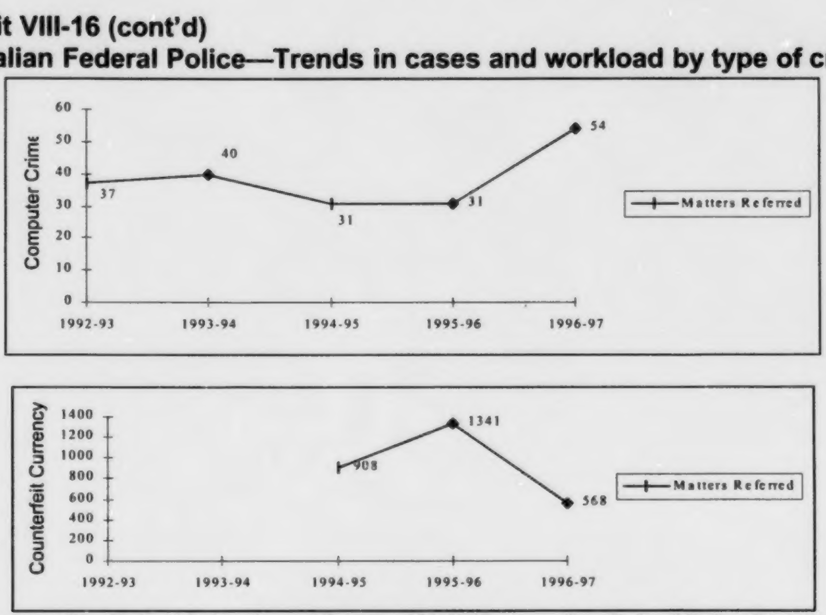


Exhibit VIII-16 (cont'd)
Australian Federal Police—Trends in cases and workload by type of crime



Source: Australian Federal Police Annual Reports, 193-1997; Australian Federal Police Situation Reports, 1993-1997.
Note: "New matters referred" means the number of incidents referred to the AFP during the particular financial year.
"Total matters initiated" means the number of incidents in relation to which investigative action was commenced during the financial year. It includes investigative action on incidents referred during the particular financial year and incidents referred during previous financial years.
"Total matters on hand" means the number of matters from the particular and previous financial years which have not been completed. A "completed" incident is one in relation to which the AFP does not expect to take further action.
"Total matters completed" refers to the number of incidents in relation to which a determination has been made in the particular financial year that the AFP does not expect to take any further action.

It is our understanding that the AFP is undergoing a restructuring to provide to specialties in:

- ***Serious fraud:*** The investigative capacity will include specially qualified officers expert in a broad range of disciplines. These officers will develop a close working relationship with a range of agencies.
- ***Fraud liaison:*** Greater emphasis will be placed on determining the law enforcement needs of client agencies and developing closer working arrangements.

- ***New forms of international crime:*** Including computer-based crime and serious environmental crime.
- ***Organized crime:*** The AFP will maintain its focus in this area and will actively assist another government authority's coordination role.

c) Federal Bureau of Investigation (FBI)

We requested budget information from the FBI. However, they informed us that their budget information could not be discussed outside of the U.S. Government as it is not public information. We were able to obtain only limited information on their resource allocations.

The FBI has now initiated the National Infrastructure Protection Center which consists of 125 government employees dedicated to protecting the nation's critical infrastructures such as electricity, telecommunications, government services, gas and oil, transportation, banking and finance, emergency services and public water systems. This office also manages computer crime investigations.

The FBI has over 500 pending computer crime cases, an increase of 300% from less than 125 only a year ago. They maintain that this number is increasing rapidly. Their budgets and staff dedicated to computer crime investigation is on the increase and will continue to grow during the next five years. For example, there are currently more than 70 Special Agents devoted to computer crime investigations, and they expect this to double within two years. They have seven dedicated computer crime squads which will grow to 12 in a year. They report that computer crime arrests have increased 900% in the last two years, which they attribute primarily to dedicated computer crime investigators.

d) Metropolitan Toronto Police Fraud Squad

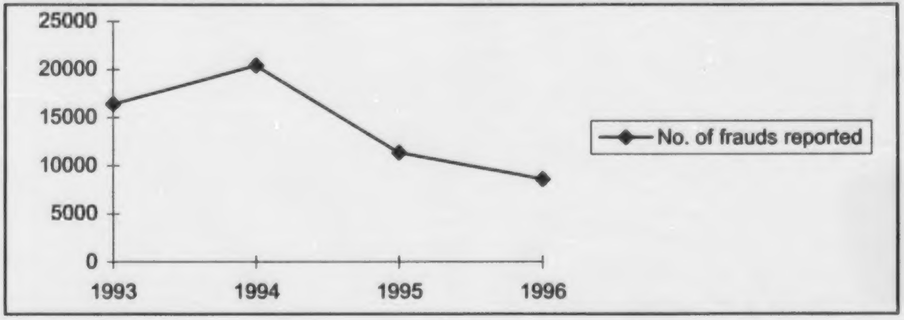
The Metropolitan Toronto Police Fraud Squad is responsible for, among other duties:

- Leading, conducting, or supporting the investigations of major fraud occurrences, political corruption, corporate crime (including real estate and stock market violations), organized electronic currency and cheque frauds and major public frauds involving large numbers of victims.

- Coordinating the investigations of minor fraud occurrences at the field level, counterfeit money occurrences and social service fraud occurrences at the field level.

Exhibit VIII-17 shows trends in the volume of reported frauds. Although these statistics do not show an increase, they should be viewed with caution. It is our understanding that the means by which statistics are gathered is misleading as to the total amount of fraud. For example, one telemarketing scam with 5,000 victims is counted as one crime. However, one person passing 100 bad cheques will be shown as 100 crimes if reported by the various victims. The downward trend is also attributable to a decrease in counterfeit currency occurrences from 9,658 in 1994 to 1,943 in 1995.

Exhibit VIII-17
Toronto Metropolitan Police Fraud Squad—Trend in Frauds Reported



Source: *Fraud Squad Review, Metropolitan Toronto Police, November 1996.*
Note: *Volume for 1996 is estimated number of year-end occurrences.*

Exhibit VIII-18 shows the trend in caseload of the Squad (as of March 9, 1998).

Exhibit VIII-18
Metro Toronto Fraud Squad—trend in assigned fraud cases by year

Year	#
1991	195
1992	151
1993	111
1994	132
1995	119
1996	79
1997	136
1998*	150

Source: FIAT System, March 6, 1998 Query, Fraud Squad. Headquarters only.
** Estimate*

Telemarketing investigations represent some 20% of the cases worked on through the years.

The current resource allocation for the squad is summarized in Exhibit VIII-19. The squad does not produce information on level of effort for cases.

The Squad recently reviewed its operations and made recommendations in the area of resource allocation. Key points of the operational review included:

- A recommendation for an **overall increase of almost 90%** in the staffing requirements for the squad. This includes:
  - **An increase in the number of civilian staff, from 3 to 7** positions recognizing the need for investigators to be working in the field rather than performing the clerical functions required for case preparations. It was reported that Fraud Squad investigators currently spend a significant amount of time carrying out clerical duties as a result of disclosure responsibilities. This administrative task should be completed by civilians trained in case preparation, document management typing and related tasks. The proposed case preparation unit would produce professional briefs, transcribe notes or tapes, complete witness will says, photocopy, enter documents into a new scanning system and provide the investigators in the unit with clerical support.
  - **A redeployment in the overall number of investigators.** Overall, an increase of 22 investigators is proposed over the current level of 29. This is to avoid overlap and to be more

cost effective. The changing nature of fraud to a global and cross border operation suggests centralization of resources.

- **Introduction of document management systems to improve performance.** Fraud Squad members will be using the Case File Program as a major incident management system in applications where the primary concern is the management of a large investigation or a series of linked investigations. The software has not yet been used by all members. The squad is now studying the potential for a document management system.
- Increased accountability of members for their own caseloads.
- Increased liaison with other police jurisdictions such as the RCMP and the OPP.

Exhibit VIII-19
Resources: Metro Toronto Fraud Squad

Positions	Budget or Expenditures	Available Days For Police Work	Approximate Annual Investigative Case Load Per Investigator
▪ Central - 1 Manager - 54 Investigators - 2 Polygraph examiners (central squad) - 2 Accountants - 3 clerical staff ▪ Field - 37 Officers (in 17 divisions) Numbers reflect implementation to date of staffing level recommendations.	▪ $ 5.5 - $ 6 million in total, of which roughly $2.9 million is in the field	▪ Field: 180 days @ 10 hours per day ▪ Central: 210 days @ 8 hours per day	▪ 5 - 6 cases ▪ For organized gangs section, trying to decrease the time of investigations to 6 months maximum

e) Ontario Provincial Police Anti Rackets Section

The Anti Rackets Section investigates enterprise crimes[18] and provides specialized investigative assistance to OPP locations, municipal police and provincial government ministries. It includes investigations of fraudulent schemes, fraud upon the Ontario Government, political/judicial corruption, computer crime, credit card fraud and proceeds of crime.

---

[18] *Enterprise crimes includes a complicated, risky undertaking or scheme, carried out in c purposeful manner, whether by false pretenses, deceit, falsehood, other fraudulent means, theft or other corrupt practices, for financial or personal gain to the detriment of persons, businesses, financial institutions or the government.*

Exhibit VIII-20 summarizes the resource allocation for the Section.

Exhibit VIII-20
Resources: Ontario Provincial Police Anti Rackets Section

Positions	Budget or Expenditures	Available Days For Police Work	Approximate Annual Investigative Case Load Per Investigator
▪ 2 Managers ▪ 77 Investigators ▪ A pool of 10 clerical staff are multifunctional, within the Criminal Investigation Bureau, but none are assigned specifically to the Anti-Rackets Section	▪ Salary: roughly $5.0M ▪ Operating: roughly $ 1,500K ▪ Roughly $100K annually for technology for 56 staff	▪ 160 - 180 days	▪ 6 - 8 cases ▪ Objective is to do a major portion in a short time but may take two years elapsed time.

Exhibit VIII-21 presents case volume and workload information for the Section. With the exception of cases for the OPP Bureau and Detachments, there is significant variability in the volume and hours required for the cases. Cases for the OPP client appear to require, on average, between 80-86 hours.

Exhibit VIII-21
Ontario Provincial Police Anti Rackets Section Investigation statistics by client type

	1994		1995		1996 (to December)	
Client	#	Hours	#	Hours	#	Hours
Federal Government	8	1,717	13	1,926	4	236
OPP Bureau and Detachment	160	13,757	159	12,701	165+	13,964
Provincial Ministries and Agencies	363	73,405	462	45,346	220+	40,047

Source: OPP Summary of Occurrence Statistics-Anti Rackets Section—Criminal Investigation Bureau.

It is estimated that there are 100-125 new cases annually. About 10% are cheque and credit card fraud, with the remainder being white collar crime.

The Section uses, at a minimum, the following methods to manage resources:

- Guidelines for a consistent assessment relating to the acceptance and assignment of new cases. This includes (1) case acceptance criteria and prioritization criteria; and (2) a policy for assigning cases to investigators based on the complexity and nature of the case.
- Case management techniques and methodologies. This includes weekly review of case progress by investigation Team Leaders and status reports by investigators.
- Use of forensic accountants under contract as in-house accountants, as members of the team.
- Migration to an investigative team concept.
- Accountability of the team leader and investigators on the team for their own cases.
- Monthly monitoring and validation of financial expenditures. Team leaders are accountable for their budgets.

2. Observations relating to resourcing from stakeholder and foreign police organization interviews

Our interviews with and reviews of documentation from stakeholders and foreign police organizations provided several observations concerning resourcing, as discussed below:

- ***Increased use of senior administrative staff for case preparation and document management:*** Crown attorney offices, regulatory body investigation teams and other police organizations have been transferring some activities formerly performed by investigators or lawyers to high level clerical staff. The role of support staff is widening from clerical duties to providing assistance to investigators. These organizations generally require one such support staff member per ten investigators.
- ***Forensic accountants key team members***: Whether they are in-house staff or contracted out, forensic accountants are integral to investigation teams. It is our understanding that the Serious Fraud Office increased their in-house staff of accountants. It has also made use of private sector accountants as teams in support of major investigations and for the purpose of acting as expert witnesses. It recognizes that the private sector accountants allows the office to have flexibility for dealing with

sudden surges in demand for forensic accounting work generated by a fluctuating workload. The Australian Federal Police proposes a new operating model with investigative teams to include specialists support such as accountants. Many of the stakeholders commented that the Program should make increased use of forensic accounting support.

- ***Technology investments for working efficiently and effectively:*** Technology is important not only to support investigators, but also to support the administrative requirements of conducting investigations. The SFO has embarked on a major project to use image-based document management systems. The aim is for a document imaging, indexing, management and storage service for material that the office seizes or receives in relation to cases. It will index and analyze that material and prepare it for court and for disclosure, and ultimately transform how the Office investigates cases. Document scanners and notebook computers for investigators, are also recognized by the OPP as important technology resources.

- ***Resources needed for proactive work:*** More than ever resources are required for public education, cooperation with other jurisdictions and crime prevention.

- ***Increases in FTEs for investigation driven by increases in caseloads and MLAT requests:*** Many of the stakeholders with whom we spoke indicated that their own investigative or prosecutorial resources had increased recently to meet caseload requirements, with percentage increases ranging from 2% to 650%. Increases in MLAT requests have been identified as a key factor in increases. The Serious Fraud Office, for example, noted a doubling of caseload for requests for assistance over a one year period.

3. Resource requirements

This section presents our estimates of the resource requirements in terms of Full Time Equivalents (FTEs) and financial resources required for the RCMP Economic Crime Program. It also includes some observations relating to economic crime cases. Our methodology, assumptions and results are included as Appendix H.

a) Approaches for generating resource requirements

Exhibit VIII-22 summarizes the resource requirements for the workload to conclude cases created in a given year and other required support over the next five years. These include the FTEs currently assigned to the Program. It is important to mention here two of our assumptions that have a direct bearing on the resource requirements. First, we have excluded any deterrence effect which could decrease the incidents of economic crimes. Thus, in the medium to longer term, the requirements may level off. Second, we have assumed that any increases in economic crime growth rates will, in turn, increase the volume of new cases at the RCMP by the same amount. These growth rates may not be achieved if complainants turn to the private sector or regulators for their investigations.

Exhibit VIII-22
Economic Crime Program Resource Requirements
1999 through 2003

Year	FTEs				Financial $(millions)
	Investigators	Management	Support	Total	
1999	695	125	97	917	$102.41
2000	738	130	102	971	$98.87
2001	791	137	108	1036	$105.40
2002	855	145	115	1115	$113.43
2003	935	155	124	1215	$122.43

Note: Numbers shown may not correspond exactly to figures in Appendix H due to rounding.

We believe these are reasonable requirements for the program. We considered estimates generated by three methods:

- **"Best guess" estimates from Commercial Crime sections.** In our consultations, we asked section heads to estimate the resources that would be required to handle the current caseload and caseload that would arise if stakeholders provided additional files to the section (unmet current demand for investigations). The estimates from the field did not take into consideration growth in criminal activity and any consequential increase in caseload. Neither did this method explicitly consider the complexity of the caseload. In the aggregate, 794 full time equivalents would be required, comprised of 722 management and investigator positions and 72 support positions. We believe that these are the minimum FTE resources required.

- **Estimates of future workload which take into account projected annual growth rates for economic crimes (and, therefore, new cases) and case complexity using a planning model** based on:

- **Concluded cases to date.** The number of investigative hours required to conclude cases in the future is calculated by examining trends and patterns over time in the complexity and level of effort to conclude cases. The volume of future new files is estimated using the growth rate. The number of investigators to meet the caseload is obtained by dividing the total investigative hours required by the amount of investigative hours per member. Because this model focuses on the historical distribution of concluded cases it is inherently "backward looking". It also does not handle determining the resource impact of backlogs from previous years. We used this model to obtain preliminary projections but did not refine it for the final resource projections.

- **The level of effort to conclude a case opened in a given year.** This is a "forward looking" approach. It can potentially show if the level of effort is increasing or decreasing over time. Also, this method can identify changes in the nature of the caseload over time, e.g. whether incoming cases becoming more complex based on trends in the proportional distribution of simple, medium and high complexity cases. As in the previous model, the volume of future new files is estimated using the growth rate. Also, the number of investigators to meet the caseload is obtained by dividing the total investigative hours required by the amount of investigative hours available per member. Ideally, 3-5 years of complete information should be available to have good information on the distribution of cases and the level of effort required to conclude simple, medium and high complexity cases. We had good information on the trend in the number of cases opened each year. However, we had only limited information on the level of effort and distribution of caseload for simple, medium and high complexity cases. In accordance with file retention requirements, data for cases concluded in 1993 was purged. There was reasonably good information on case complexity distribution and level of effort for cases that opened in 1994. Our model took these data issues into consideration. Using this approach, we estimate that 917 full time equivalents comprised of 820 management and investigator positions and 97 support positions would be required in year one for the projected workload. By the fifth year, 1090 management and investigator positions and 124 support positions would be required, a total of 1215 full time equivalents.

b) Other considerations

- **Support to the Mutual Legal Assistance Treaty (MLAT)**—In 1996 and 1997, Economic/Commercial Crime investigators provided help to overseas investigators under mutual legal assistance legislation (MLAT). These were investigations related to fraud (credit card, other and securities fraud; corruption and bribing government officials; corporate and personal bankruptcy); and other areas such as other federal acts, theft over $5k and forgery. We only have limited information on the extent of this assistance. According to the MISIII system, there were 23 MLAT files created in 1996 and 31 files created in 1997, representing a growth of 35 per cent in one year.

  We cannot say for sure if this is the total volume of MLAT assistance files. These files have only been identified since 1996 using a survey code. Investigators must be conscious to identify the survey code to the file. Hence, the volume and any percentage increase is uncertain—both could be higher or lower.

  The Serious Fraud Office in the U.K. reported that their assistance under mutual legal assistance legislation has increased sharply in 1996/97 over 1995/96. The number of requests accepted increased 95% from 35 in 1995/96 to 57 in 1996/97. Other stakeholders felt that the trend in MLAT requests is stable.

- **Assistance**—Economic Crime Program staff are providing assistance in a number of areas. These include: security and reliability inquiries, federal, provincial and municipal warrants, federal, provincial and municipal summons; Privacy and Information Act requests; order in council appointments; checks of various kinds (company, property); unspecified assistance and visits for the general public. The predominant assistance files are: Human sources (informants); company subchecks and other checks; warrants; summons; suspicious persons/vehicles; and unspecified assistance to the general public.

  It is our understanding that for most of these files, there is no requirement that the Economic/Commercial Crime investigators work on these files. We also understand that there is no screening criteria for assistance files. Some of these files could be handled by other units such as GIS. We recommend that screening criteria be developed to help decide which unit should handle assistance files.

- **Internet Crime/Computer Search**—Tech crime investigators have been participating in investigations of various sorts that have an internet crime or computer search requirements. Predominantly, these survey codes are associated with computer hacking investigations. These investigations include (in the area of economic crime) fraud, theft of telecommunications, unauthorized use of computer, credit card fraud. In areas outside of economic crime they include: morals, assault, other sex offences and cocaine trafficking.

  Like MLATs, internet crime/computer search is not an investigation class. Again, we have only limited information available on the extent and investment in this area. This type of assistance is identified through a survey code identified to the file. This code has only recently been set up in 1996 and it is our understanding that it is likely not being used as often as it should. According to the MIS/III system, there were 16 files in 1996 and 122 files in 1997, representing a growth rate of 600 percent in one year. However, we can conclude neither that this is the total volume of internet crime/computer search files nor that these are the true volume and percentage increases. There may be some support required to other investigation areas but the magnitude is extremely difficult to measure. The program manager should monitor support to these areas outside the mandate.

- **Mandate Assessment**—We were not able to make specific conclusions in this area that relate to resource requirements. It is clear that the RCMP would continue to work on medium and high complexity investigations. We believe that some portion of new cases involving simple investigations may be foregone and that these cases would be referred to provincial or municipal police services for action. However, the information available does not enable us to put a scope on this portion. We understand that, where there is a federal mandate (such as for federal laws and acts), the RCMP would continue to work on all investigations. The recommended "national interest standard" includes a criterion for action in response to the emergence of an apparent new risk or criminal approach, which may result in low, medium or high complexity investigations. For these cases, there will be the demand and necessity for the RCMP to be involved from deterrence, national interest and internal training perspectives. Accordingly, we cannot make an estimate of any savings that would result from activities that would result from application of the recommended national interest standard. We have indicated that the "Program and Case Priorities" group should make a decision on whether software piracy and copyrighting offence should be included in the mandate. As this decision is yet to be made, we have not included any estimates of resource requirements that may result.

- **Backlog**—We defined backlog, for the purpose of this analysis, as (for each year in 1994 - 1997) the difference between the cases created and cases concluded. These volumes were readily available. However, it was more difficult to assess the resource requirements impact of this backlog. Our methodology for estimating the resource requirements for backlog is described in Appendix H. Based on the information available and our assumptions, our analysis finds that to conclude the cases currently open for those years, roughly 1,437 FTEs for one year are required to clean up the backlog.

Year	Total Cases Created	Total Backlog*	% Created Cases in Backlog	% of Total Backlog
1994	3500	350	10.0%	17.5%
1995	3098	353	11.4%	17.7%
1996	2853	476	16.7%	23.8%
1997	3596	818	22.7%	41.0%
Total	13,047	1,997	15.3%	100.0%

**Note: backlog for bankruptcy, hacking and corruption excludes cases that have been concluded in 1998.*

The table shows that ten percent of cases in 1994 have not yet been concluded. This is a surprising number considering the percentage for the 1997 cases. This could be because cases are being held open for court, and in this case, the backlog is caused by delays in the court system. Other cases could be in various stages of completion. The information currently available on MIS III (that we saw) does not readily show the status of backlog cases. It is important to know this status to allocate resources. The Program should consider a backlog monitoring mechanism to show cases that are:

- In progress (being investigated).
- Completed (investigation is complete, but awaiting charges/court/prosecution).

  - Closed (investigation complete but case not prosecuted/other retribution).

  - Concluded (prosecution complete).

Knowing this information can also improve work practices. For example, it is useful to know why cases that have been investigated have not bee prosecuted.

c) Reasonableness of the resource projections

We were not able to obtain a definitive statement of the current level of resources for the program. These discrepancies are largely due to vacancy considerations and timing. There is movement in and out of the Program. Information from Finance suggests that in 1997/98, there were 475 FTEs associated with the program. Information from Commercial Crime section heads suggests that there are 487 staffed positions. Information from NHQ Program Management suggests that there are 507 positions, but many of these are vacant.

The incremental requirement of 410 resources over the current level in the first year and some 700 resources by the fifth year seems huge. However, this magnitude is more understandable when we consider the:

- Growth rates for economic crime, especially the:

  - Potential for a major crime problem resulting from the movement towards an information-based economy and the rapid growth of electronic commerce. This is clearly stated by the FBI in their 1999 budget request. Our projected volumes of new cases are built on rates of growth for economic crime. We have projected a significant rate of growth for fraud which takes into account the estimated/presumed growth rates for telemarketing fraud, internet/electronic commerce fraud, and corporate fraud as well as other fraud.

  - Potential for illegal electronic intrusion into public and private sector computer networks. This is another area of concern addressed in the 1999 FBI budget request. We have projected a significant rate of growth for computer hacking cases.

  - Increase in the volume and value of trading on Canadian stock exchanges. As markets become "hotter", the incidence of fraud increases. We have used average rates of growth in value and volume as a proxy for the trend in securities fraud, and hence, new cases.

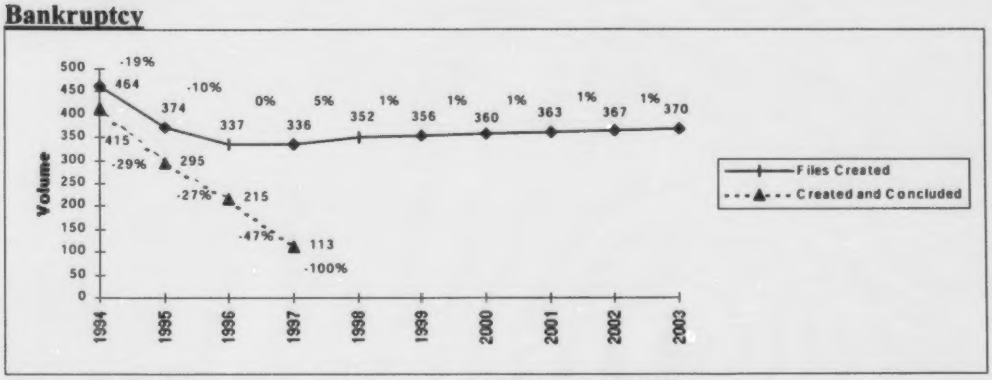
  - Growth in the number of instances in the use of fraudulent payment and credit cards.
  - Increasing technical capabilities of counterfeiters to replicate security features on Canadian and U.S. bank notes. The availability and accessibility of this technology is becoming easier and cheaper. The total volume of counterfeit notes has been increasing at over 30% per year since 1992.

- Increasing complexity of cases, through natural evolution, and the changing nature and globalization of organized criminal activities. New organized crime groups and types of criminal activities are emerging. Additionally, there is an increasing cross-border presence. More complex cases require more resources to conclude.
- Need for increased program management and policy development to: strengthen and operationalize strategic direction; develop consistent, national guidelines; conduct research and statistical analysis of current and future trends in Economic Crime; implement quality assurance; partner and liaise with stakeholders; and manage resources.

d) Observations relating to files

In preparing our models, we reviewed data from OSR/MIS III for different classes of economic crime. Here are some observations concerning their nature that should be considered in resource planning. Our observations are based on files that were resident in the system. We also show recent activity in files created and of those files, the number concluded, and the projected volume of new cases over 1999 through 2003 based on our assumptions. The gap between the two lines represents backlog, as defined in this study.

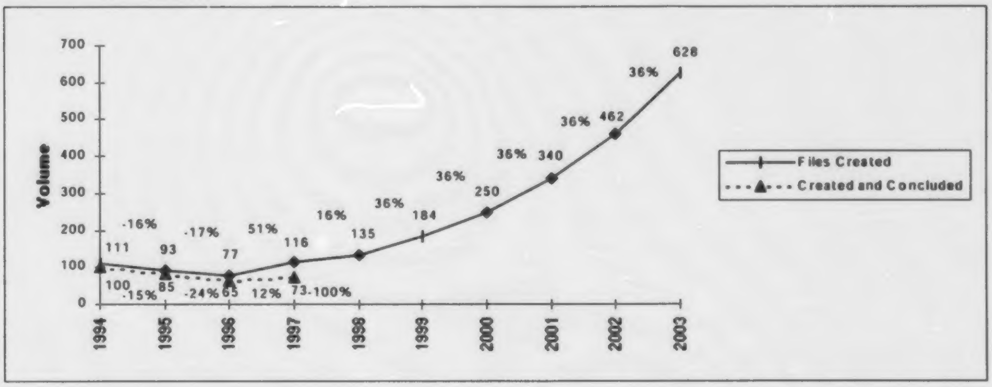
Bankruptcy



Source: RCMP MIS III reports. Includes cases concluded to end of 1997.

Bankruptcy: To date, these files predominantly been characterized as medium to complex. They can be resource-intensive. Complex files created in 1993 have required on average 3,000 hours of effort to conclude. Many of these files were open for a duration of three to four years. Our analysis indicates that 473 files created since 1994 have not yet been concluded. Most of these are type 3 cases and most were opened in 1996 and 1997.

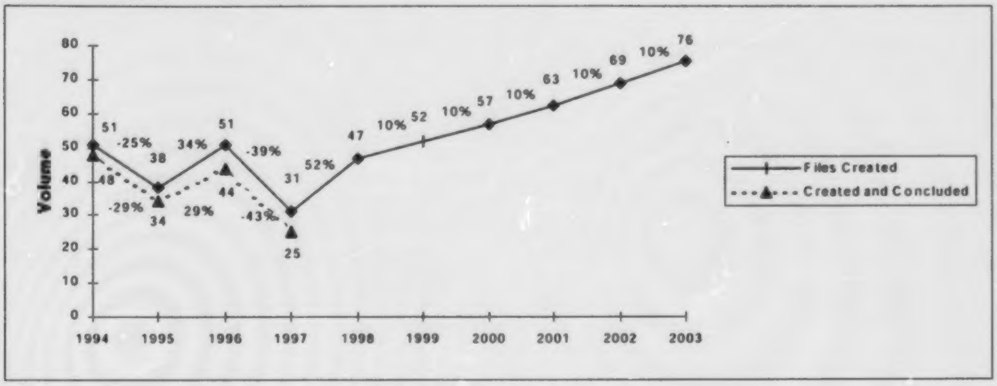
Computer Hacking



Source: RCMP MIS III reports. Includes cases concluded to end of 1997.

Computer Hacking: Overall, these files have a shorter duration and require moderate resources. Most are class 1 or class 2 complexity. We believe that 74 files created since 1994 have not yet been concluded, and that these are type 3 cases, based on the data available. Some 20 files created in 1994 and 1995 are not concluded.

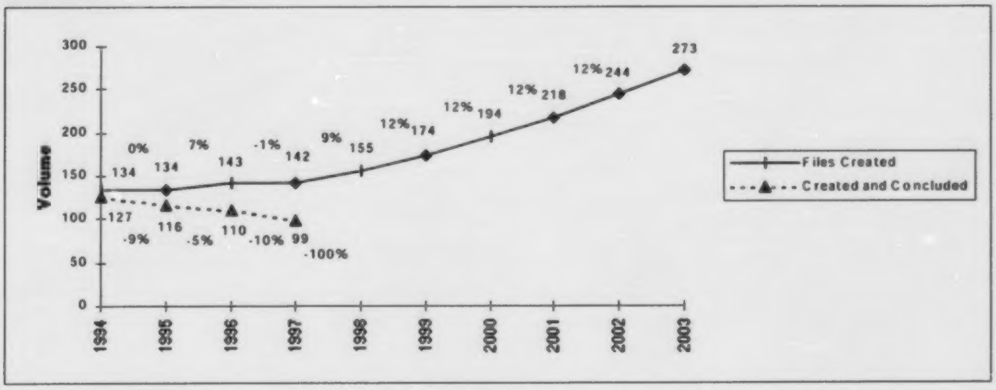
Telecommunications Theft



Source: RCMP MIS III reports. Includes cases concluded through 5/98.

Telecommunications Theft: There are relatively few of these cases to date. They are most often simple to medium complexity cases. When cases are complex, they may require around 2,000 hours of effort on average. Duration of these cases is relatively long—both medium and high complexity cases may require 2-3 years to conclude. Twenty files created since 1994 have not been concluded. We believe these include type 1, 2, and 3 files. One-third of these were opened in 1994 or 1995.

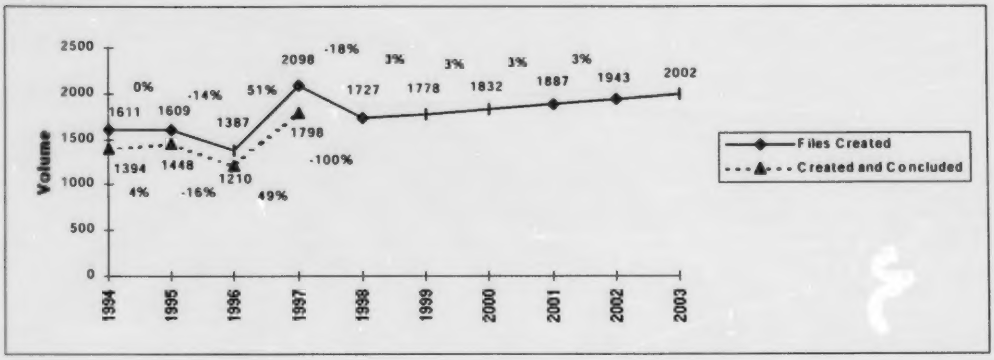
Securities



Source: RCMP MIS III reports. Includes cases concluded through 5/98.

Securities: Most of these cases are simple to medium complexity. However, there are exceptional complex cases that require in excess of 10,000 hours to conclude. With these exceptions, complex cases typically take 2,000 or so hours of effort. The data indicates that 101 files created since 1994 are not yet concluded. These are primarily type 3 files and most were opened in 1996 and 1997.

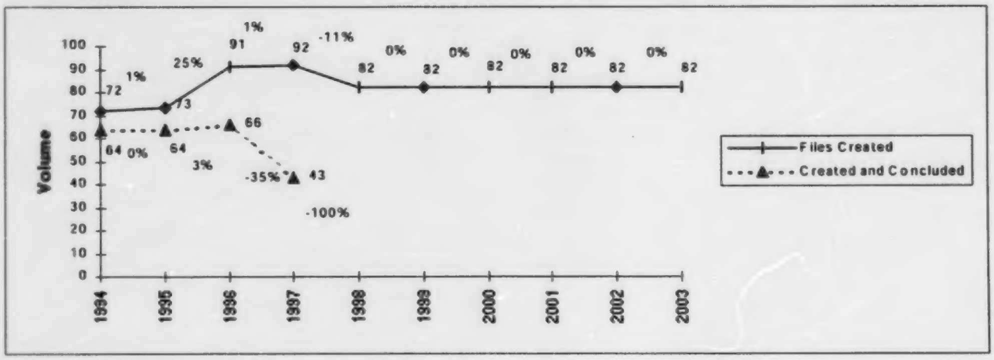
Fraud



Source: RCMP MIS III reports. Includes cases concluded through 5/98.

Fraud: These files are overall complex, resource intensive and have significant durations. There is an overwhelming proportion of files that are class 3, thus requiring over 480 hours of effort. Several files in class 3, required upwards of 12,000 hours to complete. These files tended to have durations of 3 to 6 years, though some were completed in roughly a year. The older the backlog, the greater likelihood it is a type 3. The data indicates that 855 files opened since 1994 have not yet been concluded. Almost 25% of these were opened in 1994. We believe these represent type 1, 2, and 3 files.

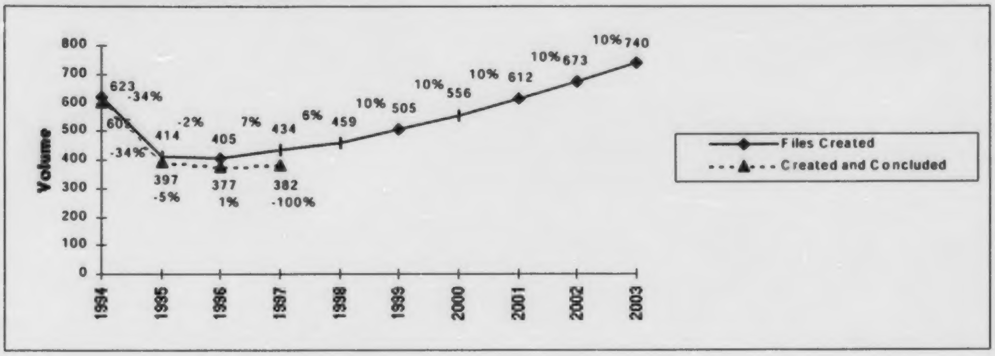
Corruption



Source: RCMP MISIII reports. Includes cases concluded to end of 1997.

Corruption: These files require moderate resources and tend to be class 1 or class 2. Complex files tend to require upwards of 1,200 hours. Most files have a duration of two years or less. There are 91 files created since 1994 that are not concluded. Most were opened in 1996 or 1997. We believe these represent type 1, 2, and 3 cases.

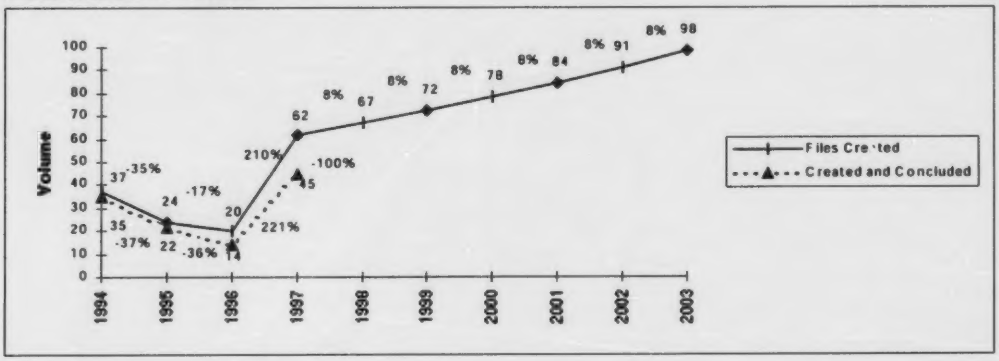
Currency Counterfeiting



Source: RCMP MISIII reports. Includes cases completed through 6/98.

Currency Counterfeiting: The overwhelming majority of these files are simple. Many of the complex files opened between 1991 and 1994 have required two to four years to conclude. Most complex cases have required on average 2,000 hours, but there are a handful of exceptional cases requiring upwards of 10,000 hours. Of files opened since 1994, 115 are not yet concluded. While most are for files created in 1997, there are a substantial number of cases opened in 1994 and 1995 that are still open. Most, we believe, are type 3 cases.

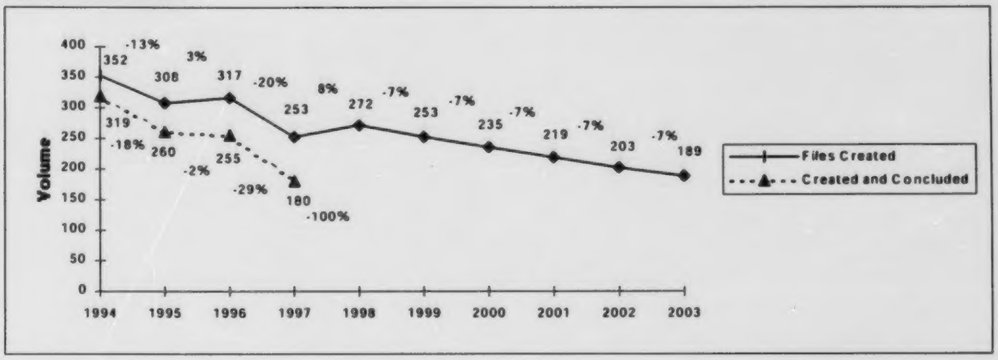
Payment Card Fraud



Source: RCMP MISIII reports. Includes cases completed through 6/98.

***Payment Card Fraud*:** To date, there have been only a handful of these cases. The data suggests that most cases have been medium complexity and have been concluded within a year. There are 27 files created since 1994 that are still open, though most of these were opened in 1997. We believe that the open files are type 2 and 3 files.

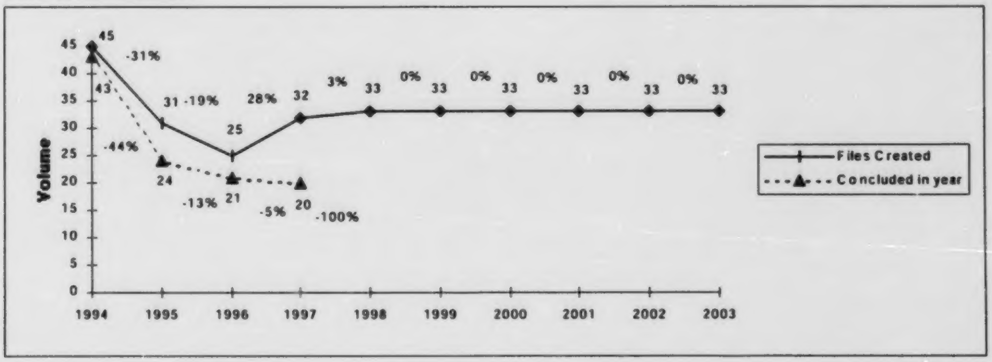
Other Offences



Source: RCMP MISIII reports. Includes cases concluded through 5/98.

Other Offences: These files seem to have, overall, moderate complexity with a concentration of more complex files requiring 1,500 - 7,000 hours. Many complex files have timeframes of 2-4 years. The data indicates that there are 216 files created since 1994 that are still open. They occur in 1994 through 1997. We believe they represent type 1, 2, and 3 cases.

Federal Statutes



Source: RCMP MISIII reports. Includes cases concluded through 4/98.

Federal Statutes: There have been, in recent years, only a handful of these cases. They are mostly simple cases with some that are medium complexity.

Though they are not complex cases, they have been requiring 2-3 years elapsed time to conclude. Twenty-five of the cases opened since 1994 have not yet been concluded. We believe they represent a type 1, 2, and 3 cases.

e) Offence activity

A file can represent effort towards multiple offences. For example, an individual file can be investigated for bankruptcy and fraud charges. Appendix I shows trends in the volume of activity for offences. Thus, the "fraud" chart shows all the files with a fraud offence.

The resource requirements presented in this chapter are dependent on a set of specific assumptions and the information analyzed. Any modification to our assumptions and/or the analytical framework will change the projections. The workload projections take into account other components of our study, namely, the impact analysis, key themes from our consultations with stakeholders and members, and the proposed organizational structure. The resource requirements presented are those for the projected annual volume of new cases. We must also note that we have provided projections of resource requirements—not resource allocations. We have not distributed the requirements across periods (e.g., months or quarters) or years.

We have not attempted, as it is not our role, to incorporate changes in case acceptance and prioritization criteria, mandate, etc. as these proposals have yet to be accepted and designed definitively by Program Management. Nor have we attempted to say what resources would be obtainable. We are concerned that, in the short term at least, the Program (and the RCMP) will not be able to recruit, train, operationalize and manage the incremental resources. Accommodation for these incremental resources is just one example of potential capacity limitations. Even though we have proposed a recommendation to set up a National Economic Crime Program/Service Line, many facets of the Program must continue to operate within the context of the RCMP.

Economic Crime Program Management must assess the capacity of the RCMP to handle recruitment, staffing, training, technology procurement and installation and accommodation. Also, there are several systemic issues that must be addressed as well for the Program to meet its challenges. Program Management must consider the extent to which these issues can be addressed in the short term. The next step is the preparation of a business case for obtaining resources. The business case must consider these assessments and show adjusted resource requirements. It should also consider the resources that would be available from stakeholders such as corporations and regulatory bodies. A proactive national approach should be developed for approaching stakeholders and discussing resourcing matters. As well, the business case should address resource allocation matters such as how the resources would be distributed across time periods. Resource allocation is dependent on performance standards that must be set by Program Management in areas such as the duration of cases, staffing of cases, treatment of backlog, etc.

Increasing resources is not a panacea for the Program challenges that we have discussed in earlier chapters. There is no doubt that more resources will help address some challenges but, unless these resources are managed effectively and appropriately trained and equipped, they will not produce significant, sustainable benefits. The incremental (and the current) resources must be managed and monitored to ensure that they are allocated where they are required the most, based on the Program's priorities. A solid business plan with ranked priorities and clear and measurable objectives and outputs is a prerequisite for managing and obtaining resources. Before providing resources, government and stakeholders will want to know that the resources they provide will be managed and used for achieving key objectives and outcomes. They must also have the assurance that management is accountable for how the resources have been used, especially if objectives have not been met.

We also cannot emphasize enough the need for monitoring how resources, once allocated, are being used. New approaches and tools are needed. An approach that reviews the status and phases of each case is necessary to monitor progress (and hence, backlog). Potential phases for cases could include: not assigned; assigned - investigation not started; investigation in progress; investigation complete - referred to prosecutors for action; awaiting trial; completed - no prosecutorial action taken; concluded. Consistent performance standards should be set for these phases and for the complexity levels of cases. Progress would then be measured against the standards. Case complexity classes should be further refined. There are many complex cases in excess of 480 hours. We suggest setting up additional classes for high level of effort, for example: 480 - 5,000 hours; 5,000 - 10,000 hours; greater than 10,000 hours. With refined levels, workload projections will have more accuracy. Finally, case status and resource investments (effort and financial) must then be monitored on an on-going basis, and corrective action taken immediately, where necessary, to get cases and budgets back on track.

F. Resource management policy issues

There are several questions that the Economic Crime Program policy centre should address relating to on-going resource management:

- ***Can the profile of white collar crime be raised sufficiently to attract the public's and therefore government's attention?*** Raising the government's awareness/attention in the short and intermediate term is seen as a prerequisite for obtaining additional resources for the Program.

- ***Should the investigation of frauds internal to corporations, or other offences that result from insufficient control/governance mechanisms be financed by public monies?*** Implementation and application of the National Interest Test (NIT) could address this issue.

- ***Can the Program afford to investigate some offences (e.g., theft of telecommunications <$5K; thefts from coffee money in federal government departments)?*** Theft of telecommunications <$5K is an offence under the Technological Crime services of the Program's mandate. Similarly, financial theft where the federal government is the victim is a mandated area of the Federal Statutes and Programs service. Again, for theft of telecommunications, the National Interest test should be applied. If a complaint does pass the NIT and any other criteria, the next step is to determine whether the complaint should be investigated by internal or external resources.

- ***Will there be sufficient resources in the prosecutorial function to handle increased output from Commercial Crime?*** This is an important issue. Investing resources to increase the number of investigations and outputs by the Economic Crime Program does not seem to be beneficial if cases are not able to be brought to trial. At a minimum, increased investigation may have a deterrent effect. The Program policy centre should consult further on this with the Crown prosecutors to determine where, and to what extent, the potential increased prosecutorial workload is an issue.

IX

Recommendations

The main recommendation of this report pertains to the implementation of the preferred organizational model for the Economic Crime Program, which was described in detail in Chapter VIII. The present chapter consolidates the other recommendations resulting from the various study components. We suggest that these other recommendations be implemented in order for the RCMP to a achieve a fully functional and effective Economic Crime Program.

A. Impacts of economic crime and stakeholders' expectations regarding the future positioning of the Program

Our research indicates that the total estimated magnitude is significant – at least $2.1 to $3.1 billion, plus currently unknown losses to emerging, hard-to-value crimes like Internet fraud and computer crime. Of this amount losses by individual consumers and investors amount to about $0.6 - 1.6 billion, and losses by enabling organizations amount to about $1.5 billion. These amounts should be viewed as "best guess" estimates for the most part, given that they are based on expert opinion and extrapolations from data that often cannot be validated, or validated with great difficulty.

The impacts of these losses extend from the losses and disruption to individual consumers and investors to reduce revenues and profitability for enabling organizations to reduced levels of tax revenue and higher program payouts for the federal government to distortion of the monetary data and economic signals used by economic policy makers. Ultimately, these impacts have the potential to damage the integrity of our economic infrastructure and to erode public confidence, in both Canada and internationally, in the safety, security and integrity of the infrastructure.

Stakeholders indicated to us that they believed the Program no longer has the resources required to carry out its mandate. Consequently, they have had to take remedial action of their own to remedy the problems created by this resource gap, as listed below:

- Needs to expand monitoring and investigation activities by enabling business and public service organizations.
- Loss of deterrence effects.

- Limited capability to respond to the increasing number of national and international crime activities.
- Extended time periods for investigations and low probabilities of conviction.
- Increasing reliance on administrative penalties and civil remedies, with declining success in controlling activities of organized crime groups.
- Rising popularity of Canada as a base for certain types of international economic crime.
- Unmet needs for proactive intelligence gathering and dissemination.

We are of the opinion that, in order for the Program to maximize the impact of any increases in the resources made available, it will need to focus on areas where the magnitude of impacts can be maximized, working in partnership with other stakeholder organizations. Feedback from our stakeholder interviews pointed to a need for the following focus in the Program's strategies and operations; we support these suggestions:

- Cases involving organized crime groups that account for significant losses or disruption. In other words, "go after the big guys, and send a strong deterrence message to the little guys."
- Cases that have national and international components, and are typically more complex and require higher levels of technical expertise, which is often not present in provincial or municipal police forces.
- Cases that respond to emerging new threats and risks, in order to slow the spread of new criminal approaches and ensure the Force stays "ahead of the game.
- Providing leadership and coordination, through the development of a stronger intelligence capability and the sharing of information with relevant stakeholders, leading to a more proactive approach to combating economic crime.

B. Recommendations relating to the national role and interests

Several primary objectives were set for our work that had a bearing of the definition of the Program's mandate and setting of operating priorities. Our recommendations regarding these study objectives are summarized below.

1. Definition of the "national role and interests" of the Program

This primary objective required us to clearly define what is meant by the "national role and interests" of the Economic Crime Program. Our recommendations on this objective relate to:

- The definition of the national interest in law enforcement.
- The identification of economic crime activities that affect the national interest and fall within the purview of the Program
- The criteria to be used in the Program's "national interest standard".

We propose that the national interest in law enforcement relates to:

- ***Protection of the integrity of the national economic infrastructure***, which involves both private and public sector infrastructure providers.
- ***Maintenance of public confidence in the integrity and safety of the economic infrastructure***, spanning its component market structures and transaction systems, as well as the integrity and equity of federal revenue (e.g., tax collection) and social (e.g., Employment Insurance) programs. Public confidence, in this sense, relates to the confidence of the Canadian public generally and in the public's roles as consumers and investors, plus the confidence of international customers and investors.
- ***Maintenance of public confidence in the integrity of public management and political oversight of the functioning of government.***
- ***Maintenance of a flexible and competitive economy***, such that law enforcement requirements are balanced against needs for commercial responsiveness and competitiveness.
- ***Efficient resource management to optimize expenditures on law enforcement*** across all jurisdictions and types of stakeholders (law enforcement agencies, regulatory agencies and enabling business and public service providers).
- ***Consistent approaches to law enforcement*** involving economic crime incidents across Canada.

Any type of economic crime has the potential to affect the national interest, especially if they are largely ignored by law enforcement agencies, primarily through their ability to weaken public confidence in the integrity of Canada's economic infrastructure. Information from our external and internal interviews, and findings from our literature review, indicate that the following economic crime activities are likely to have the greatest impact on the national interest in law enforcement:

- Crime activities that:
    - Involve organized crime groups that account for significant losses or disruption.
    - Involve large scale, systemic fraud, computer crime or other types of economic crime.
    - Have regional, national and/or international dimensions.
    - Require higher levels of expertise and specialized knowledge to investigate, due to their complexity.
    - Respond to emerging threats and risks.
- These activities are not mutually exclusive, which is one reason why they are most closely linked to the protection of the national interest in law enforcement.

Based on the above findings, we recommend that the Program incorporate a revised "national interest standard" into its mandate, as shown in Exhibit IX-1.

Exhibit IX-1
Recommended "national interest standard" for the Program

The Economic Crime Program undertakes investigations, and related activities, in which one or more of the following factors are present:

- ☐ Involvement of organized crime group(s).
- ☐ Large scale systemic fraud, involving a large number of victims and/or a significant financial risks or losses.
- ☐ Complex:
  - Involving a high degree of criminal sophistication;
  - Requiring a high degree of investigative and/or technical expertise; and
  - National or international in scope.
- ☐ Widespread (regional, national or international) public concern or interest in combination with political interest or the potential thereof.
- ☐ Emergence of an apparent new risk or criminal approach, with potential for rapid diffusion, or significant financial risks or losses, if left unattended.
- ☐ Opportunity to achieve a strong deterrence effect, either by sending a message to criminal groups or encouraging greater caution on the part of consumers and/or investors.
- ☐ No scope for administrative penalties of civil actions, or such approaches are proving to be ineffective.
- ☐ Action required under the terms of an existing treaty, agreement or memorandum of understanding with other law enforcement agencies, regulatory agencies or industry groups representing the interests of enabling business organizations within the economic sector targeted by the criminal activity.

A "Program and case priorities group" composed of a small number of senior Program managers (e.g. Director, officer(s) in charge of various crime groups and regional managers) is also desirable, to resolve questions regarding the assessment of certain cases and to regularly review the working of the national interest standard and results achieved by the Program.

2. Recommendations relating to the extent to which Canada and the U.S. must harmonize their enforcement efforts

The RCMP is being called upon by many stakeholders to increase its level of participation and visibility in harmonization initiatives, and to serve as a focal point nationally for transborder economic-crime law-enforcement discussions. The RCMP, with its national scope and mandate, has the unique ability to serve as a key contact point for Canada/US and multilateral negotiations and discussions in this area. Direct participation of RCMP representatives in talks will be important to ensure that public commitments made are realistic and that sovereign control over economic crime law enforcement on Canadian soil can be properly maintained. Increased RCMP prominence at the international negotiation table will also serve to rebuild the RCMP's credibility and image in the economic crime field.

As the world enters the Internet era, law enforcement must be capable of reacting quicker than ever before, building solid cases based on evidence synthesized from multiple sources inside Canada and abroad. Canada's current laws and policies were, for the most part, conceived and adopted at a time before "high tech" crimes (with thousands of geographically-scattered victims) became prevalent. Given this dramatic change in context, the RCMP must work proactively with the respective Justice Departments as well as with other partner agencies across Canada and the US to adapt to and to shape a modernized law enforcement environment and to develop a "North-American response" to key economic crime problems.

C. High-level recommendations on Human Resources Management

Throughout the course of the study, a number of Human Resources Management (HRM) issues came to light. These HRM issues, however, were not restricted to the Economic/Commercial Crime Program, but were systemic problems within the Force. Of particular concern to Economic/Commercial Crime were such issues as:

- The inability of Economic/Commercial Crime to attract and retain appropriately skilled staff.
- Lack of career path/stream within Economic/Commercial Crime.
- Hierarchical promotion methods/inability to reward strong performance.

In order to achieve the requirements and potential inherent in a National Economic Crime Program, these issues need to be addressed. Simply supplementing the program with additional resources will not suffice. The National Economic Crime Program must advocate for changes to current Human Resources Management policies, particularly regarding how they affect the potential ongoing success of the proposed national program model.

Below we provide some very high-level conceptual recommendations regarding HRM practices and recommend the National Economic Crime Program lobby Senior Management and the Human Resources Department strongly in the following areas.

1. Specialization

Ever-increasing criminal sophistication dictates that as a national police force, the RCMP can no longer regard all its crime programs as generalist in nature. This type of generalist mentality, that any member can/should be able to perform any set of duties well, is no longer applicable. The skills required to perform generalist duties such as highway patrol are not the same as those skills and knowledges required to investigate a securities fraud on one of the Canadian Stock Exchanges or track down an organized crime group perpetrating credit card fraud. Some programs within the Force (e.g., Ident, Economic Crime, etc.) should be set up as "specialized" programs. The National Economic Crime Program requires individuals with not only general competencies, skills and knowledge but also additional skills and knowledges specific to the program (e.g., business management knowledge, accounting knowledge, legal skills, technological skills, etc.).

2. Staffing/recruitment

Good Human Resources Management practice dictates that in any HRM process, Line/Operational Managers and Human Resources Specialists have specific sets of responsibilities. Line/Operational Managers identify problems or needs and use Human Resources Specialist expertise to help them address these problems/needs. Human Resources Specialists provide expert advice, guidance, design processes in support of effective management decision-making, provide statistical and analytical support, etc. However, they do not make any final decisions with respect to the ongoing management of people and programs.

The recruitment and staffing process is an example of just such an HRM process. Accepted staffing/recruitment practice outlines Line/Operational Manager and Human Specialist responsibilities as follows:

Management

- define program requirements
- identify need for resources
- define selection criteria
- **make final decision on selection method (e.g., transfer, hire, secondment, contract, etc.)**
- **make final decision on successful candidate(s)**

Human Resources Specialist

- provide advice on selection criteria
- provide advice on recruitment/ selection method, suggest alternatives
- assist in identifying candidates
- present candidates and assist in selection process

The final decision must always remain with operational manager who has identified the need. Human Resources Specialists perform a key function in the process but only in the role of expert advisor and consultant, never as final decision-maker.

3. Career streaming/succession planning

Not only must "specialized" programs attract appropriate and qualified candidates to perform the work, these programs must make a significant investment in the recruitment and development of these resources. Therefore, to maximize return on investment, it is not cost-effective to maintain a high turnover rate. To that end, a specialized program such as the National Economic Crime program should provide a viable and flexible career path to retain qualified members and facilitate effective succession planning. A national program such as the model proposed could provide ample opportunity for members to obtain a variety of career experiences both in the field as well as at Headquarters. Setting up different levels within position types similar to a classification system would allow members to progress upward as well as lateral through the Program to get additional experience and knowledge.

4. Classification/promotions/reward-recognition

Throughout our study, "ranking" of positions was highlighted as a major problem. Members are currently unable to progress within the Commercial Crime program unless a higher ranked position were available. Therefore, many excellent investigators who would have liked to remain in Economic/Commercial Crime have been forced to leave in order to obtain a promotion. It was suggested, to address this situation, that all positions within the new structure be established as "Person Year Exempt Category" (PYEC) positions. This is not a viable solution. The PYEC process is used for the creation of specific positions required for a finite period. To that end, the process should not be used to circumvent the current established system of "ranked" positions for a particular program such as Economic Crime. Instead, to address the problem for "specialized" programs, the current ranking system should be reviewed in detail and alternative systems assessed to allow for more flexibility.

To manage such "specialized" programs as the National Economic Crime Program, two possible options exist at the conceptual level for these programs.

Option 1

Make all positions within the program "special agent" status. Create job categories, evaluate them, create salary ranges and allow members to progress through the ranges or be promoted through the levels within a category of positions.

Option 2

If the "rank" system were to be maintained, set up a parallel specialized rank structure. In addition to the existing rank system (e.g., constable, corporal, sergeant, etc.), create specialized ranks (e.g., constable-s, corporal-s, etc.) similar to the military model, which would reflect the specific technical knowledge and skills requirement for specialized programs. Evaluate these types of positions in relation to more generalist ranks and allow progress/promotion through the ranges for specialized ranks.

Both options would allow for an increased capability to retain expertise and reward members appropriately.

D. High-level recommendations of Resource requirements

In order for the Economic Crime Program to meet its mandate and to address emerging challenges, it must be equipped with sufficient resources. This translates into having the appropriate levels of human, financial and technical resources to operate the Program effectively.

To establish and maintain a successful National Economic Crime Program, we recommend the following resourcing strategies.

1. Establish an overall approach to resource management

In addition to identifying what types and amounts of resources are required, the Economic Crime Program must also establish an effective approach to managing the resources. The overall approach should encompass four key components:

- **Establish a resource management framework** to address the Program's overall resource management system and to establish an appropriate accountability framework. Such a framework allocates and supports the control of and the accountability for resource management and consumption between headquarters and the field.

- **Determine resource requirements** based on the activities performed by the program using appropriate/accepted approaches to estimate requirements.
- **Determine long-term strategies for obtaining resources** through the identification of both traditional as well as new sources of funding for mandated activities and services. Suggestions on both short and long term strategies to consider are provided in Chapter VIII.
- **Manage the resource allocation process** to ensure the appropriate infrastructure is in place to assign, manage and monitor the efficient and effective use of allocated resources. Key areas to address are highlighted in Chapter VIII. Monitoring the program performance against objectives to allocate and reallocate resources is a key need.

2. Follow a set of resource allocation and management principles

To improve overall resource management for the program, KPMG recommends that:

- NHQ Program Management develop a clear statement of objectives and ranked priorities for the Program (which are consistent with high level departmental direction). The Commercial Crime Section management should participate in identifying and assessing, collectively, the Program priorities. These statements can then be formulated in a Program Business Plan.
- Based on the priorities and objectives, develop and assign budgets.
- The Program Management establish a mechanism for management to discuss and agree to resource allocations and re-allocations.
- Establish mechanisms for consulting with stakeholders and clients on a regular basis to assess demand and resources required.

3. Establish and fund an effective training strategy

On-going learning and development will be critical to maintain adequate knowledge and skill levels for all Economic and Tech Crime investigators. A focussed strategy is needed so that on-going skills and knowledge requirements for all positions can be set, current skills and knowledge levels can be identified and the learning gap can be measured and addressed. A variety of training options should be identified, analyzed, costed and included in an on-going learning and development plan.

Training funds should be allocated and controlled effectively to address the most critical learning gaps required to ensure on-going and effective Program operation.

4. Technology is a critical resource

Technology is a critical resource particularly for Tech Crime investigators. Tech Crime investigators need to have the technology to enhance their productivity and capability to investigate both technological crime and provide investigative support to technologically-assisted crime investigations.

As well, Economic Crime investigators should have appropriate technological support tools to facilitate their investigative work.

The technology standard for tech crime and economic crime investigators must be set. Technology funds should be allocated and controlled effectively to ensure that members and staff who require the technology are able to obtain it.

5. Increase Economic Crime Program resources over time

An analysis of resource requirements, based on the information available and using a workload planning model and incorporating necessary support indicated that, over time, more resources will be required to conclude an increasing caseload. Changes in assumptions will clearly change the projections.

Merely increasing resources will not enable the Program to meet the challenges addressed in our document. These resources must be managed and monitored to ensure that they are allocated where they are required the most, based on the Program's priorities. A solid business plan with ranked priorities and clear and measurable objectives and outputs is a necessity.

X

Implementation Approach

NOT INCLUDED

Appendices

A. List Of Participants in Individual Interviews or Group Consultations (NOT INCLUDED)

B. RCMP Mandate For Economic Crime

C. Organizational Design Principles

D. Other Organizational Options Considered

E. Possible Sub-activities

F. Senior Experts on Transnational Organized Crime:
40 Recommendations from Lyon G8 Conference

G. Guiding Principles For Resource Allocation And Management

H. Resource Requirements Methodology And Assumptions (NOT INCLUDED)

I. Offence Activity Volumes

J. Bibliography

Appendix A

List Of Participants in Individual Interviews or Group Consultations (NOT INCLUDED)

Appendix B

RCMP Mandate For Economic Crime

RCMP Mandate For Economic Crime

A. Preamble

The RCMP has an obligation to respond to economic crime where the interests of the Government of Canada and Canadians are at stake. Because of its national and international presence; its role in the preservation of national interests; its ability to co-ordinate the gathering and dissemination of criminal intelligence; and the fact that stakeholders have expressed a collective need for its involvement, the RCMP is well suited to conduct certain types of investigations.

It has long been acknowledged that when RCMP federal resources are conducting interprovincial or international investigations, that will ultimately be prosecuted under the Criminal Code, the deployment of federal resources to conduct these investigations is considered acceptable. In cases where federal RCMP resources are used to conduct provincial Criminal Code investigations, care must be taken to ensure that all economic crime investigations satisfy a "national interest" standard.

The RCMP Mission Vision Values statements make it clear that the RCMP must provide the highest quality service through dynamic leadership, education, and technology in partnership with the communities that we serve. All RCMP Economic Crime Program personnel are firmly committed to these important principles. As a result of this commitment, the RCMP has often been heralded as a leader worldwide in these areas and its technical and investigative expertise and experience in specialized law enforcement are widely recognized and respected.

B. Organization for delivery

1 The Economic Crime Program comprises the Economic Crime Branch (Federal Services Directorate) at the National Headquarters level and Commercial Crime Sections at the Division level.

2. Economic Crime Branch is responsible for program management.

3. Divisions are responsible for the delivery of the Economic Crime Program and should direct resources in accordance with the broad parameters set out in the

following mandate. A certain amount of flexibility will permit Divisions to properly address local issues, concerns, and priorities.

C. Defining the mandate

The Economic Crime Program is committed to leadership and excellence in the delivery of the following police services and in developing related crime prevention strategies:

- Commercial Fraud
- Federal Statutes and Programs
- Technological Crime
- Securities Fraud

1. Commercial fraud

- To investigate economic crimes of a national or international significance (having due regard for contractual obligations with the provinces) in which one or more of the following elements are present:
    - Organized crime involvement
    - Substantial value or financial losses
    - High degree of criminal sophistication
    - Requirement for special investigative expertise
    - Municipal or provincial governments as victim
    - Satisfying public or national interest
- To provide assistance to international law enforcement agencies relating to economic crimes in accordance with established MLAT obligations.

2. Federal statutes and programs

- To investigate criminal activities relating to the bankruptcy and insolvency process and to co-operate with the Superintendent of Bankruptcy.
- To investigate economic crimes such as corruption, fraud, or financial theft cases where the Government of Canada is the victim.
- To investigate the following types of technological crimes of a national or international significance pursuant to the Criminal Code:
    - Bank Act
    - Income Tax Act
    - Financial Administration Act
    - Small Business Loans Act

- Canada Elections Act
- Parliament of Canada Act
- Farm Debt Review Act
- Investment Canada Act
- Tax Rebate Discounting Act
- Employment Insurance Act
- Currency Act

3. Technological crime

- Offences relating to the counterfeiting of currency (e.g., bank notes, coins, tokens of value) as set out in Part XII of the Criminal Code;

- Offences not included in Part XII of the Criminal Code but involving the manufacture, possession, and/or distribution of counterfeit or altered payment cards, cheques, bonds, or other negotiable instruments;

- Offences where computers and/or the contents of computers are the object of a crime (e.g., Unauthorized Use of Computer and Mischief to Data); or

- Offences relating to the theft of telecommunications (e.g., Theft or Telecommunication Service and Possession of Device to Obtain Telecommunication Service) in which one or more of the following elements are present:

  - Organized crime involvement

  - Substantial value or financial losses

  - High degree of criminal sophistication

  - Requirement for special technical or investigative expertise

  - Satisfying public or national interest

- To provide support in computer-assisted crimes involving economic crime offences (e.g., fraud or theft) where the computer is used as a tool to facilitate the commission of an offence. Other non-program offences committed using the Internet or other computer and telecommunication devices (e.g., drug trafficking, smuggling of immigrants, or the distribution of child pornography) will normally be referred to the law enforcement agency or RCMP unit having primary jurisdiction or responsibility for investigation.

4. Securities fraud

- To investigate market manipulations with an emphasis on those cases of a national or international significance.
- To investigate other Criminal Code offences relating to publicly traded securities.
- To assist provincial securities commissions and in those provinces where the RCMP has jurisdiction, to investigate provincial securities act offences.
- To investigate criminal offences relating to registered representatives or stock brokers.
- To maintain a close liaison with securities regulatory institutions with the goal of encouraging the implementation of crime prevention and community policing concepts in all securities fraud enforcement strategies.
- To gather and disseminate intelligence information and to maintain a criminal vetting system for applicants to the securities industry.

Appendix C

Organization Design Principles

Organization Design Principles

1. The organization must be able to deliver on its mandate.
2. The organization should focus on those functions that are most essential to its business.
3. The organization must be able to meet customers' requirements satisfactorily. Both internal and external customer needs should be taken into consideration.
4. The organization should be sufficiently flexible to respond rapidly to changing operational and technological needs.
5. The structure should facilitate efficient decision-making and policy implementation. This can be accomplished by reducing the number of management layers, reducing the number of process steps and hand-offs, and establishing clear lines of authority. Each level of management should have a clear rationale and necessity, with distinct and measurable value-added. Each organizational level should be marked by real and significant 'jumps' in cognitive and task complexity and responsibilities and have the appropriate skills to accomplish assigned tasks.
6. The structure should facilitate succession planning and the development of successors, as well as the development of people in general. Opportunities for advancement should be provided through lateral and cross-functional movements rather than through progression upward within a traditional hierarchy.
7. Authority and accountability should accompany the assigned level of responsibility. The structure should facilitate efficient reporting and communications. (The number of levels in the hierarchy directly affect communications and reporting.)
8. Overlap and duplication should be eliminated.
9. Functional expertise should be consolidated in specific organizational units. This will eliminate the fragmentation of responsibility and authority.
10. There should be a closer working relationship among occupational groups to facilitate both an understanding of the complexities and challenges of differing

responsibilities, and to allow for the development of individuals with a thorough understanding of the working environment and its challenges. (Requires a commitment to provide time and financial support.)

11. The organization should ensure the capacity to plan for the future. The organization should ensure that at least one unit is charged with responsibility to plan on a longer-term strategic basis, and is given the support required to sustain these endeavours.

12. The structure should reflect a balance of a centralized and decentralized nature of operations by providing for local support to operations, as well as increased local autonomy and authority.

In addition to the above design principles, the following criteria should guide implementation of the chosen option:

1. Minimization of risk that services will be adversely affected.

2. Ease.

3. Duration.

4. Cost.

5. Fit with skill sets that already exist and those needed in the future.

Appendix D

Other Organizational Options Considered

Other Organizational Options Considered

Option 1: Maintain Current Situation

- The current model has Commercial Crime investigation reporting regionally and Policy and Program Development reporting centrally to Economic Crime Branch at NHQ. Allocation of responsibilities differs across the country.

Option 2: Decentralized Model (modified status quo)

- Investigative teams would be drawn from a flexible pool of multi-skilled investigators as required for different cases. Investigators would be assigned to a specific Coordinator for administrative purposes only. Coordinators would work together closely to ensure appropriate resource allocation to projects.

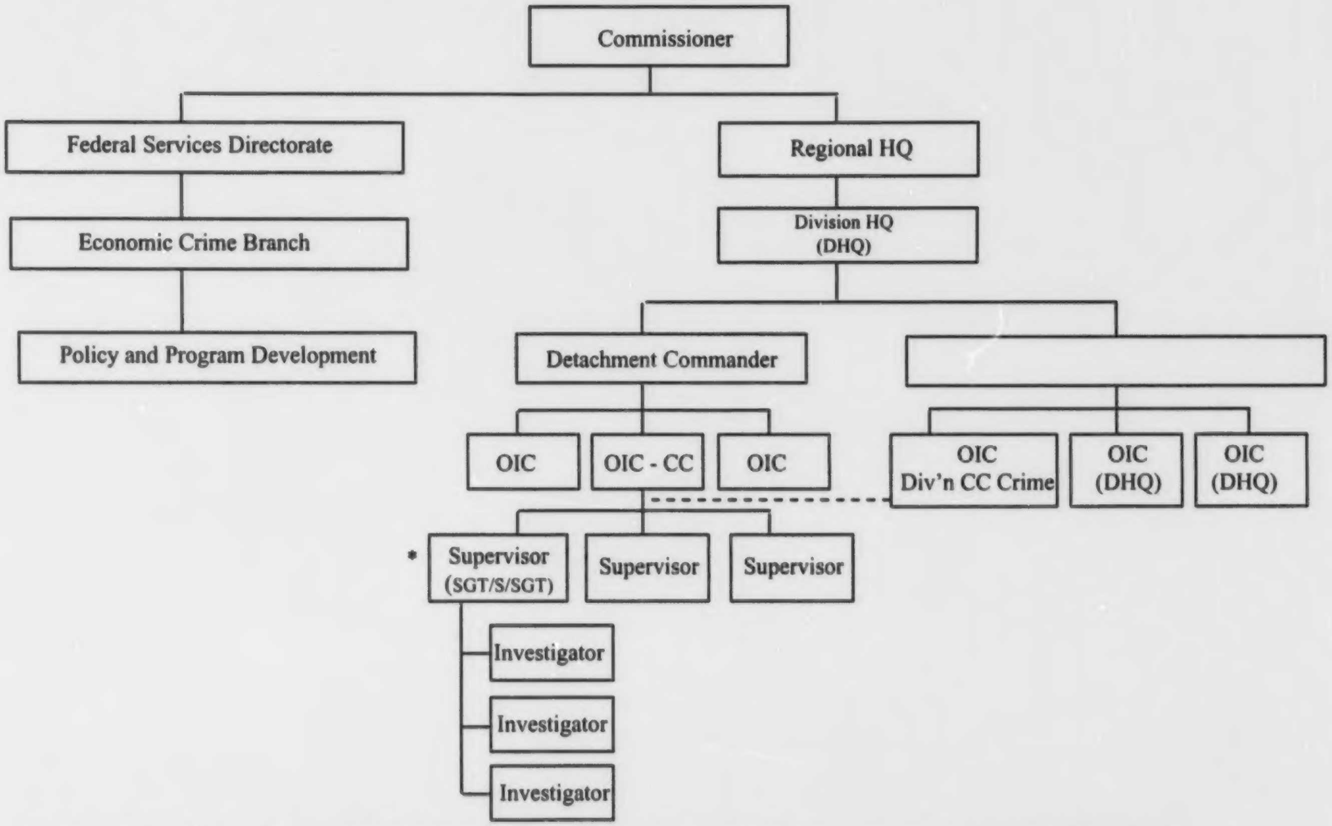
Option 3: A National Economic Crime Program (recommended option)

- Refer to Chapter VII of this report for details.

Option 4: Specialized Multi-disciplinary Economic Crime Office (external to RCMP)

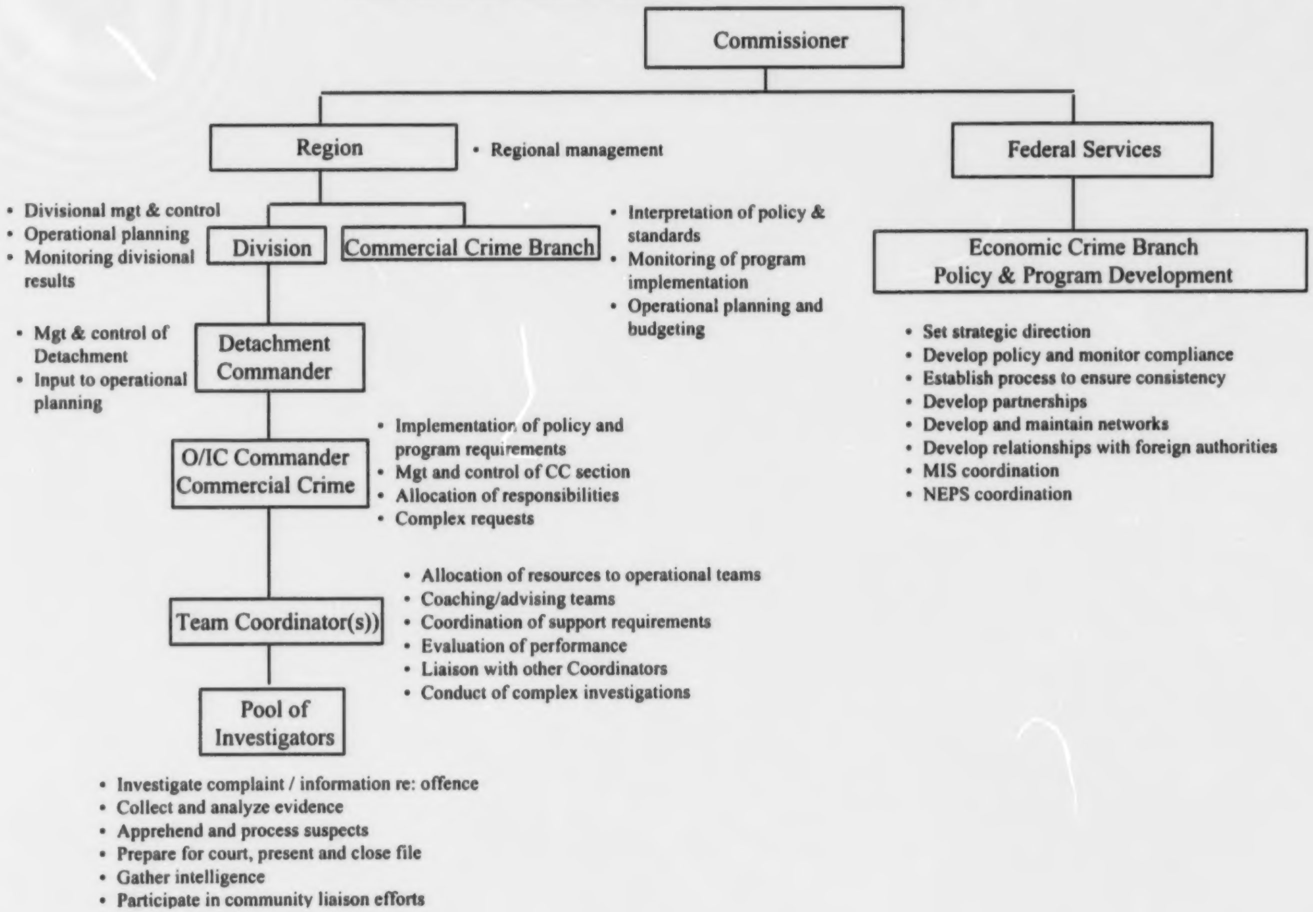
- Team Coordinators would assume responsibility for the formulation of Operational Teams to handle cases. Operational teams would be drawn from a flexible pool of multi-skilled investigators as required for different cases. Investigators would be assigned to a specific Coordinator for administrative purposes only. Coordinators would act as coaches/leaders to these drawn from a flexible pool of multi-skilled investigators. Coordinators would work together and with Investigative Support closely to ensure appropriate resource allocation to projects.

Option 1: Current Situation (Generic Diagram)


Commissioner
Federal Services Directorate
Economic Crime Branch
Policy and Program Development
Regional HQ
Division HQ (DHQ)
Detachment Commander
OIC
OIC - CC
OIC
OIC Div'n CC Crime
OIC (DHQ)
OIC (DHQ)
* Supervisor (SGT/S/SGT)
Supervisor
Supervisor
Investigator
Investigator
Investigator

* ***(Investigative units are organized differently across the country. Units can be organized by commercial crime type (e.g., Fraud, Counterfeit, Securities/Market, Tax, etc., or by jurisdiction (e.g., federal, provincial, municipal, etc.).***

Option 2: Decentralized Model *(modified status quo)*


Commissioner
Region
Federal Services
Division
Commercial Crime Branch
Economic Crime Branch Policy & Program Development
Detachment Commander
O/IC Commander Commercial Crime
Team Coordinator(s))
Pool of Investigators

Region

- Regional management

Division

- Divisional mgt & control
- Operational planning
- Monitoring divisional results

Commercial Crime Branch

- Interpretation of policy & standards
- Monitoring of program implementation
- Operational planning and budgeting

Detachment Commander

- Mgt & control of Detachment
- Input to operational planning

O/IC Commander Commercial Crime

- Implementation of policy and program requirements
- Mgt and control of CC section
- Allocation of responsibilities
- Complex requests

Team Coordinator(s))

- Allocation of resources to operational teams
- Coaching/advising teams
- Coordination of support requirements
- Evaluation of performance
- Liaison with other Coordinators
- Conduct of complex investigations

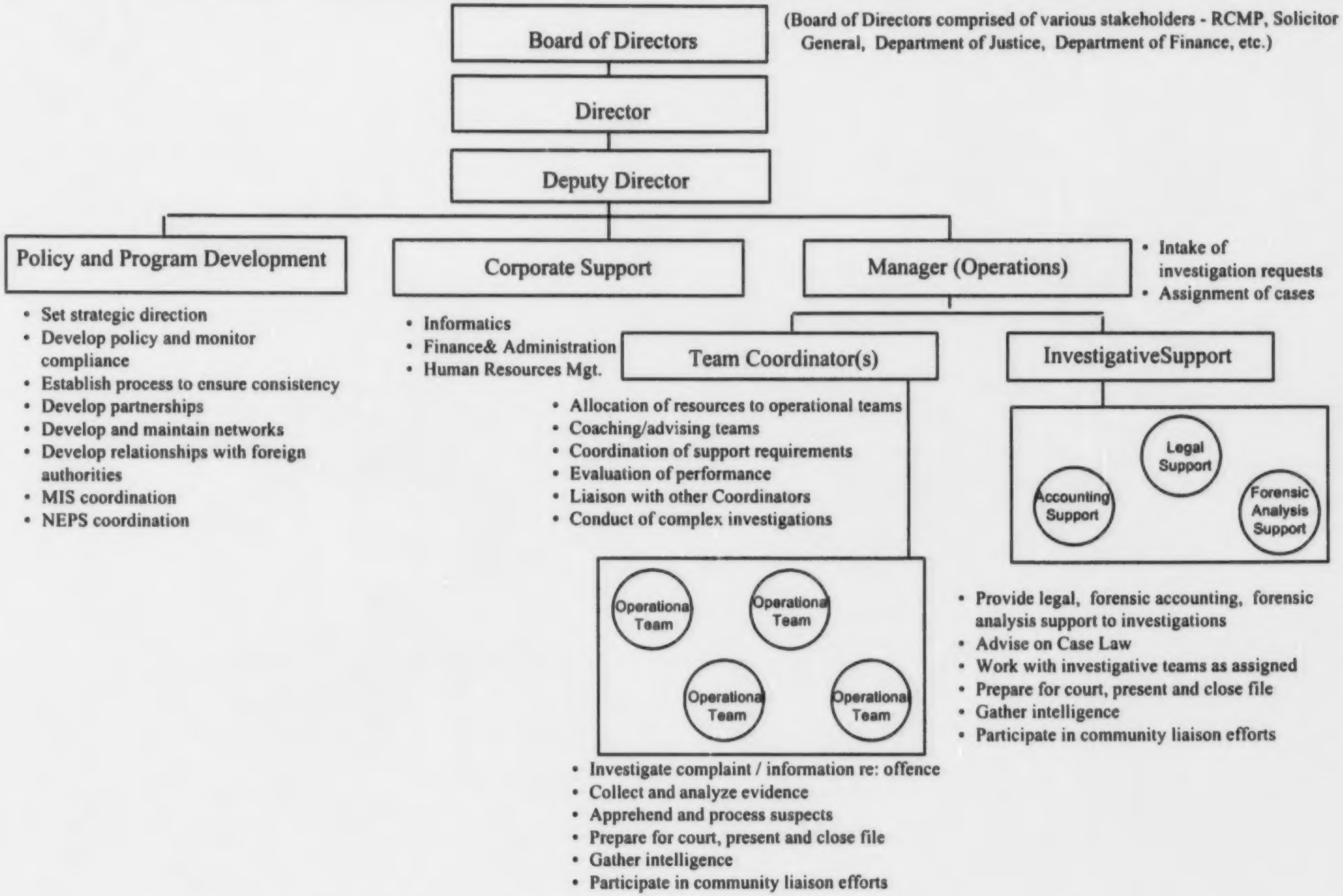
Pool of Investigators

- Investigate complaint / information re: offence
- Collect and analyze evidence
- Apprehend and process suspects
- Prepare for court, present and close file
- Gather intelligence
- Participate in community liaison efforts

Economic Crime Branch Policy & Program Development

- Set strategic direction
- Develop policy and monitor compliance
- Establish process to ensure consistency
- Develop partnerships
- Develop and maintain networks
- Develop relationships with foreign authorities
- MIS coordination
- NEPS coordination

Option 4: Specialized Multi-disciplinary Economic Crime Office (external to RCMP)



Board of Directors

(Board of Directors comprised of various stakeholders - RCMP, Solicitor General, Department of Justice, Department of Finance, etc.)

Director

Deputy Director

Policy and Program Development

- Set strategic direction
- Develop policy and monitor compliance
- Establish process to ensure consistency
- Develop partnerships
- Develop and maintain networks
- Develop relationships with foreign authorities
- MIS coordination
- NEPS coordination

Corporate Support

- Informatics
- Finance& Administration
- Human Resources Mgt.

Manager (Operations)

- Intake of investigation requests
- Assignment of cases

Team Coordinator(s)

- Allocation of resources to operational teams
- Coaching/advising teams
- Coordination of support requirements
- Evaluation of performance
- Liaison with other Coordinators
- Conduct of complex investigations

- Investigate complaint / information re: offence
- Collect and analyze evidence
- Apprehend and process suspects
- Prepare for court, present and close file
- Gather intelligence
- Participate in community liaison efforts

InvestigativeSupport

- Provide legal, forensic accounting, forensic analysis support to investigations
- Advise on Case Law
- Work with investigative teams as assigned
- Prepare for court, present and close file
- Gather intelligence
- Participate in community liaison efforts

Appendix E

Possible Sub-Activities

Possible Sub-Activities

Legend: ***P = Primary Responsibility; S = Secondary Responsibility***

	Economic Crime - NHQ	Field Mgmt	Investigators	Tech Crime - NHQ	Tech Crime Investigators
Policy & Program Development					
Set vision and strategic direction	P	S			
Develop and monitor policy/standards of practice	P	S			
Establish process to ensure consistency across country	P	S			
Develop program through partnering with other agencies	P	P			
Facilitate national and international networks	P	P			
Facilitate relationships with foreign authorities / international intelligence / covert operations	P	S			
Assume responsibility for setting and facilitating implementation of continuous learning & development	P	P		P	
Establish ongoing relationship with HR department—input to selection/staffing process, promotions, rewards & recognition, classification, etc.	P	S			
Conduct research—trend analysis/future trends and issues	P				
Facilitate receipt and dissemination of strategic intelligence	P	S		P	
Foster sharing of information/best practices across RCMP (central repository)	P	S		P	
Deal with jurisdictional issues at local, provincial, national & international level	P	P		P	
Define results to be achieved for Economic Crime Program	P	P			
Solicit input from Economic Crime local units located in the field for preparation of Business Plan, Operational Plan, and budget	P	S			
Provide input to departmental Business Plan; develop Operational Plan	P				
Set resource levels based on demand, budget available, and results to be achieved	P	S			
Monitor resource usage and results achieved, and make appropriate adjustments	P	P			
Conduct economic profiling—NEPS	P				

	Economic Crime - NHQ	Field Mgmt.	Investigators	Tech Crime - NHQ	Tech Crime Investigators
Foster "quality federal policing service delivery"/CAPRA model across Program	P	P			
Conduct research/trend analysis re: new technologies & tech crime				P	
Provide technical support to complex tech crime cases				P	S
Establish strategic linkages/partnerships with High Tech industry				P	S
Investigation					
Apply national interest test to select cases in accordance with agreed national guidelines and selection/priorization criteria and tempered by local requirement	P	P			
Intake of cases	S	P	S	S	S
Receive complaints, review/assess data prior to investigation			P		P
Prepare operational plans/methodologies to conduct investigation(s)			P		P
Investigate complaints / information about Economic/Tech Crime offences	S		P	S	P
Collect and analyze evidence			P		P
Search and analysis of data			P		P
Apprehend and process suspect(s)			P		P
Prepare for court, present and close file			P		P
Establish plans and procedures to target specific criminal populations/commodities			P		P
Gather tactical intelligence on: methodologies, procedures, tools, suspects, etc.			P		P
Conduct initial discussions/planning regarding cases with stakeholders		S	P		P
Participate in industry associations/attend conferences	P	P	P	P	P
Participate on /lead taskforces with other policing authorities at the local, national, & international	P	P	P	P	P
Share information across RCMP	P	P	P	P	P
Other					
Provide assistance to RCMP units / other police forces / government departments, stakeholder organizations (e.g., cost recovery/exchange of services, joint forces initiatives, etc.)	P	P	S	P	S
Increase awareness/image of Economic Crime through focussed communications/marketing strategy	P	P		P	

	Economic Crime - NHQ	Field Mgmt.	Investi-gators	Tech Crime - NHQ	Tech Crime Investi-gators
Participate in community relations, liaison and education/crime prevention activities (e.g., speaking engagements, committee participation, etc.)	P	P	P	P	P
Perform emergency security duties as required	S	S	S	S	S

Appendix F

Senior Experts On Transnational Organized Crime: 40 Recommendations from Lyon G8 Conference

Senior Experts On Transnational Organized Crime: 40 Recommendations from Lyon G8 Conference

Paris, April 12, 1996

P8* - Senior Experts Group Recommendations

To combat Transnational Organized Crime efficiently members recommend the following:

1. States should review their laws governing criminal offences, jurisdiction, law enforcement powers and international cooperation, as well as their measures dealing with law enforcement training and crime prevention, to ensure that the special problems created by Transnational Organized Crime are effectively addressed.

2. With the aim of improving mutual assistance, States should, as needed, develop mutual legal assistance arrangements or treaties, and exercise flexibility in the execution of requests for mutual assistance.

3. States should, where feasible, render mutual assistance, notwithstanding the absence of dual criminality.

4. States developing mutual assistance treaties should ensure that the treaties:

   a) Provide a clear description of the scope of the assistance available.

   b) Encourage a speedy process of assistance.

   c) Are as comprehensive as possible in terms of types of assistance available.

   d) Reflect the principle that evidence will be gathered in the manner sought by the requesting states, unless the procedures are contrary to the fundamental principles of the law of the Requested State. To further facilitate cooperation against Transnational Organized Crime, States should consider negotiating arrangements in areas that are not covered by Mutual Legal Assistance Treaties.

5. States should establish a Central Authority which would be structured to provide speedy coordination of requests.

   The Central Authority should provide a quality control and prioritizing function for both incoming and outgoing requests to take into account both the seriousness of the offence and the urgency of the request.

   At the same time, the Central Authority should not be seen as an exclusive channel for assistance between States. Direct exchange of information between law enforcement agencies should be encouraged to the extent permitted by domestic laws or arrangements.

6. States should prepare and distribute to other States materials that would describe the channels of communication for mutual assistance and extradition and the process for obtaining such assistance from that State.

7. In cases where a criminal activity occurs in several countries, States with jurisdiction should coordinate their prosecutions and the use of mutual assistance measures in a strategic manner so as to be more efficient in the fight against transnational criminal groups.

8. States should be encouraged to develop, through treaties, arrangements and legislation, a network for extradition. States should modernize their extradition treaties by eliminating the lists of crimes and allowing for extradition of conduct punishable in both States by deprivation of liberty in excess of an agreed minimum period.

   States should make best efforts to ensure that their domestic arrangements for extradition are flexible enough to permit extradition to States of a different legal tradition. They should seek to identify and eliminate obstacles to extradition, including those that may arise from the differences between legal systems, by, for example, simplifying evidentiary and procedural requirements.

9. States should ensure that their domestic arrangements for extradition are as effective and expeditious as possible. States should also consider the possibility of extradition without a treaty.

10. If extradition of nationals is not permitted by the Requested State, and the extradition of one of its nationals is requested, the Requested State should:

    a) Allow for conditional extradition on the condition that it is only for trial and that its national be promptly returned after trial to its territory for service of any sentence within the limits of the law of the Requested State.

b) Allow for transfer/surrender, when it is permitted by domestic law, only for trail and on the condition that its national be promptly returned after trial to its territory for service of any sentence within the limits of the law of the Requested State.

c) Apply the rule of "aut dedere, aut judicare" by, at the request of the Requesting State, submitting the case to its competent authorities in order that proceedings may be taken if they are considered appropriate.

11. States should promote other techniques for mutual education that will facilitate mutual assistance and extradition, such as language training, secondments and exchanges between personnel in Central Authorities or between executing and requesting agencies.

    Training courses, joint seminars and information exchange sessions should be encouraged on a bilateral, regional and world wide basis.

12. Consideration should also be given to posting in other States representatives of prosecuting agencies or of judicial authorities.

13. States should provide effective protection for individuals who have given or agreed to give information or evidence, or who participate or who have agreed to participate in an investigation or prosecution of an offence, and of the relatives and associates of those individuals who require protection, because of risk to the security of the person.

14. States should consider, as appropriate, reciprocal arrangements for the protection of witnesses and other endangered persons.

15. States should consider adopting appropriate measures to ensure the protection of witnesses during criminal proceedings. These might include such methods as testifying by telecommunications or limiting the disclosure of the address and identifying particulars of witnesses. Consideration should be given to the temporary transfer as witnesses of persons in custody enlargement of the admissibility of written statements, and the use of modern technology, such as video links, to overcome some of the current difficulties with obtaining the testimony of witnesses located outside the prosecuting State.

16. States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed. Liaison between law enforcement and prosecution personnel of different States should be improved, including the sharing of experience in addressing these problems. States should promote

study in this area and negotiate arrangements and agreements to address the problem of technological crime and investigation.

17. States should take all other lawful steps available under domestic legislation, to ensure that they do not provide safe havens for criminals.

18. We commend the work does by Interpol and World Customs Organization calling upon these organizations to maintain and develop their support for operational activity, facilitating as rapid as possible as exchange of information between law enforcement agencies. We call upon them to focus on a strategic overview of the methods of, and trends in, Transnational Organized Crime for the benefit of all their member countries.

19. In order to facilitate the work of law enforcement practitioners we will, on request, provide brief guides on our respective legal systems and on the mandates of relevant agencies.

20. States should identify within their existing structures central contact points for the purpose of facilitating contact between their operational agencies. It may be useful to locate these points in liaison with the Interpol National Central Bureau.

21. We stress the important contribution that liaison officers can make to the fight against Transnational Organized Crime. We encourage States to make the most effective use possible of their liaison officers in other countries and to consider additional postings. We stress the need for liaison officers to have access, in accordance with the law of the host country, to all agencies in that country with relevant responsibilities.

22. We reiterate our condemnation of drug trafficking which is a major source of finance for Transnational Organized Criminal Groups. Therefore, we: reaffirm the importance of the three United Nations Conventions (1961, 1971 and 1988) which are fundamental to action against illicit drugs, call on all States to adopt and fully implement legislation in accordance with those conventions, believe in the value of giving the widest publicity to information issued by official international bodies, such as the International Narcotic Control Board, on illicit drug production, trafficking and the proceeds of the illicit drug trade will work in all relevant fora to prevent the diversion of chemical precursors used in illicit drug production and take necessary steps to implement fully all relevant international agreements, welcome and support implementation of the recommendations of United Nations International Drug control Program working group on maritime cooperation.

23. In order to ensure more effective transnational crime prevention, and foster public safety, we will develop strategies to identify and combat the illicit traffic in firearms.

In furtherance of this goal, and in support of the specific recommendations contained in the May 1995 resolution from the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders and the July 1995 United Nationals Economic and Social Council resolution, we will, and encourage other States to, review existing firearms laws and regulations to facilitate discussion at an international level.

We will promote information exchange among our relevant law enforcement authorities. We encourage States to enhance the exchange of information useful for law enforcement purposes (e.g., data for the identification of illicit firearms and specific information on tests conducted on firearms and ammunition which have been used in the course of criminal activities.).

24. States should ensure that immigration services play their part in the fight against Transnational Organized Crime. We note the involvement of Transnational Organized Crime in alien smuggling and call upon all States to enact legislation to criminalize such smuggling of persons. Immigration services and other agencies should: exchange information on the transnational movement of organized criminals, have as full as possible an exchange of information on forged and stolen documents used by traffickers, consider the most effective means for its communication.

We will take necessary steps to improve the quality of our travel documents. We encourage other States to improve theirs and will assist them to do so.

25. We support the exchange of law enforcement expertise regarding scientific and technological developments such as advances in forensic sciences.

26. We emphasize the relevance and effectiveness of techniques such as electronic surveillance, undercover operations and controlled deliveries. We call upon States to review domestic arrangements for those techniques and to facilitate international cooperation in these fields, taking full account of human rights implications. We encourage States to exchange experiences of their use.

27. We emphasize the importance of giving the fullest possible protection to sensitive information received from other countries.

The competent authorities of different States, should advise each other as to the requirements regarding the disclosure of information in the course of judicial and administrative proceedings, and discuss in advance potential difficulties arising from those requirements.

A transmitting State may make conditions for the protection of sensitive information before deciding whether to transmit it. A receiving State must abide by the conditions agreed with the transmitting State.

28. Building on current cooperative arrangements, the different agencies in our countries will develop their work together in specific law enforcement projects targeted on Transnational Organized Crime. We have formulated practical guidance on project-based action and commend this approach to all States.

    Project-based action involves bilateral multilateral priority setting, targeting, resourcing and assessment of law enforcement operations drawing on the strength of the full range of competent agencies.

29. We welcome the Financial Action Task Force on Money Laundering to resolve to extend criminalization of money laundering to other serious offences.

30. States should consider adopting legislative measures for the confiscation or seizure of illicit proceeds from drug trafficking and other serious offences, asset forfeiture, as required, and the availability of provisional arrangements, such as the freezing or seizing of assets, always with due respect for the interest of bona fide third parties. States should also consider the introduction of arrangements for the equitable sharing of such forfeited assets.

31. States should consider implementing measures to detect and monitor the physical transportation of cash and bearer negotiable instruments at the border, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of legitimate capital movements.

32. States should adopt the necessary legislative and regulatory measures to combat corruption, establish standards of good governance and legitimate commercial and financial conduct, and develop cooperation mechanisms to curb corrupt practices.

33. We agree to share information on practical anti-money laundering techniques and to draw on the experience gained to adapt and improve national and international training activities in this area, in conjunction with the action of the Financial Action Task Force on Money Laundering.

34. In order to improve understanding and information on the detection of financial networks linked to transnational organized crime (in particular investments by Transnational Organized Crime), we encourage States to take measures to gather financial information and , as much as possible, facilitate the exchange of such information, including exchanges between law enforcement agencies and regulatory bodies.

35. We urge States to adhere to and fully implement existing relevant multilateral Conventions whose provisions effectively contribute to the fight against all forms of Transnational Organized Crime, in particular the Conventions concerning control of illicit drugs.

36. We will keep under review the possibility of supplementing existing conventions and adopting new instruments, in response to developing needs in the fight against Transnational Organized Crime.

37. We support and encourage the provision and reporting of clear and accessible information on adhesion to and implementation of the main conventions.

38. In order to avoid wasteful duplication and to ensure that limited resources are used to best effect, we urge International Organizations to coordinate their work programmes and to concentrate their efforts within their areas of competence on activities of practical value to member States.

39. We will work together in the governing bodies of International Organizations whenever possible, in order to give more coherent impetus and coordination to the fight against Transnational Organized Crime.

40. We will seek to ensure that all International Organizations that play and effective role in the fight against Transnational Organized Crime have adequate resources to fulfill their mandate. We will also examine possibilities for providing appropriate financial resources for specific, practical and viable projects developed by competent International Organizations.

Source: France, Ministère de l'Intérieur, 12 April 1996.

* P8="Political 8" (G7 + Russia)

Appendix G

Guiding Principles For Resource Allocation And Management

Guiding Principles For Resource Allocation And Management

- **Establish formal prioritization mechanisms.** Where initiatives or activities are no longer considered a priority, resource allocations should be adjusted to support the service or activity at a maintenance level. If the service or activity is no longer required, the service or activity should be phased out and those resources allocated to priority areas.
- **Allocate resources in relation to priorities.** Transfers of resources should take place through transparent mechanisms. Staff must be redeployed to new areas depending on the issues of the day or in accordance with emerging priorities. The staff should receive the necessary training to deal with priorities. A business case approach should be used to allocate resources by evaluating and prioritizing proposals and matching limited resources to priorities.
- **Resource allocation must be linked to the Department's and Program's Strategic Plan and Business Plans**. This implies that Strategic, Business, functional plans are linked. Strategic priorities, established for the program as a whole and spanning a 3-5 year planning horizon, guide the process of planning and resource allocation. A business case approach should be used to allocate resources by evaluating and prioritizing proposals and matching limited resources to priorities. Strategic priorities must be ranked or prioritized at a corporate/program level.
- **Involve Program management in resource allocation decisions.** NHQ Program management must take an active role in resource allocation and re-allocation decisions. However, managers at all levels in the Program should be held accountable for resource forecasts and consumption.
- **Operating units should have input to the definition of policy, priorities and allocation of resources.** This implies that managers should be responsible for planning, budgeting, managing and using the resources which support the activities for which they are accountable. Managers should be owners of the plans they develop. Budgets should be issued well in advance for planning purposes.
- **Emerging pressures should first be addressed through the reallocation of existing resources**. This implies that Sections should manage workload

increases within their allocated budget, and should look first to their own budgets for new (but approved and high priority) initiatives.

- **The resource allocation culture must support openness and flexibility.** Managers must be rewarded for showing flexibility in freeing up resources. They should not be penalized with lower funding levels the next year. However, there should be penalties for repeated lapsing.

- **The planning and resource allocation processes must be sufficiently flexible to respond to issues and change, yet be as simple as possible.** This implies that priority-setting, workplanning and resource allocation must be tightly integrated and seen as a single process. The Program must be sensitive to its resource impact within the department. Also, the planning process must recognize that client demand will evolve. Controls must be minimized as this can be a major demotivator to staff.

- **Resource allocation and resource usage should be transparent.** This implies that open communication must be established so plans, budgets and timetables can be negotiated with program and section management. Progress and variances against plan will be communicated on a regular basis to all managers. Managers at all levels must understand what resources are being drawn down by various projects and activities. There are surprises as to how the budget is determined. Each Section has access to information on the other Section's budget.

- **The Program should maximize its access to external funding.** This implies that the Department will petition, on behalf of the Program, Treasury Board Secretariat and client departments or stakeholders for additional resources where a valid business case exists, and where the requirements cannot be met by internal reallocation. If resources are provided by stakeholders/clients for special purposes or projects, the resources should not be available for re-allocation without client/stakeholder consent.

- **Clients/stakeholders should be involved in the resource allocation process on an on-going basis.** Clients should be consulted in the resource planning phase and on an on-going basis. The Program must be sensitive to its resource impact on stakeholders/clients. For example, reductions in resources may affect the ability to meet service standards. Additionally, the Program's planning process must acknowledge that client demand will evolve. Resource allocation must be linked to client/stakeholder demand.

- **The planning and resource allocation frameworks must address project and policy-oriented activities as well as investigation activities.** Logical, uniform and consistent approaches must be used to determine the resource requirements for similar classes of activities. Key projects for achieving Program priorities must be appropriately resourced. It must be suitable for all areas of the Program.

- **Build resource management expertise.** Management positions may need upgrading of resource/financial management skills. Also, project or team leaders may need training in project management techniques. The Program as a whole, may require more specialized financial expertise.

Appendix H

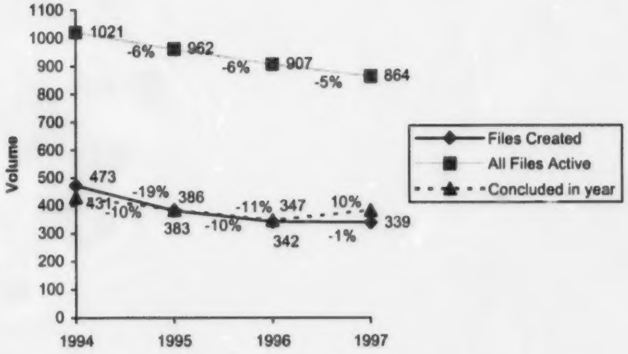
Resource Requirements Methodology And Assumptions (NOT INCLUDED)

Appendix I

Offence Activity Volumes

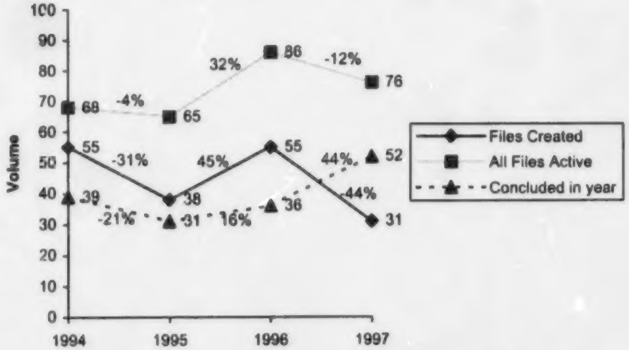
Note: Volumes indicate the volume of files referencing the designated offence types as the primary and other levels of code.

Bankruptcy



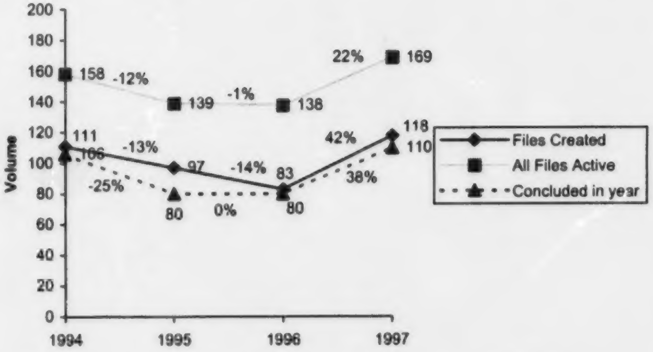
Source: RCMP Economic Crime MIS III. Query run before 4/7/98.
Represents OSR Codes: AE05 Bankruptcy Corporate; AE15 Bankruptcy Personal.

Telecommunications Theft



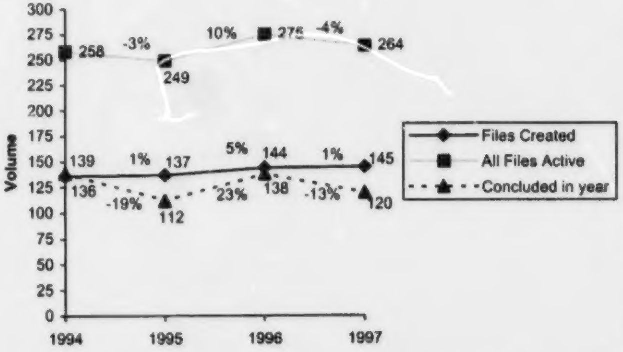
Source: RCMP Economic Crime MIS III. Query run before 4/7/98.
Represents OSR Codes: AB67 Theft of Telecommunications <$5K; AB68 Theft of telecommunications >$5K.

Computer Hacking



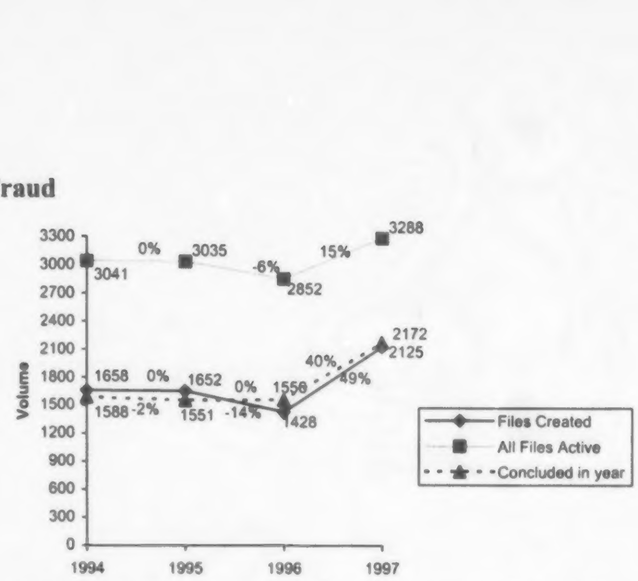
Source: RCMP Economic Crime MIS III. Query run before 4/7/98.
Represents OSR Codes: AC65 Unauthorized use of computer; AC66 Mischief to data summary offence; AC68 Mischief to data-indictable offence; DK64 Illegal decoder.

Securities



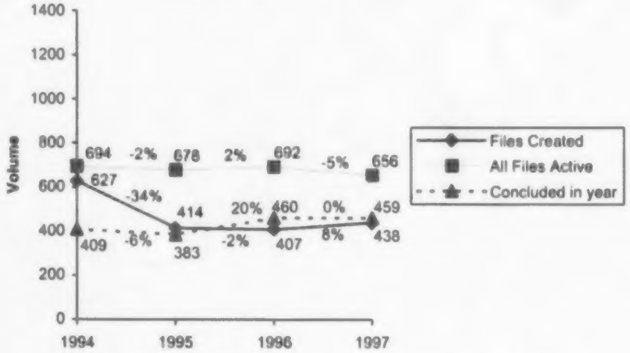
Source: RCMP Economic Crime MIS III. Query run before 4/7/98.
Represents OSR Codes: AB56 Securities fraud; AB66 Stock market related offences; AG10 Securities Act (Provincial).

Fraud



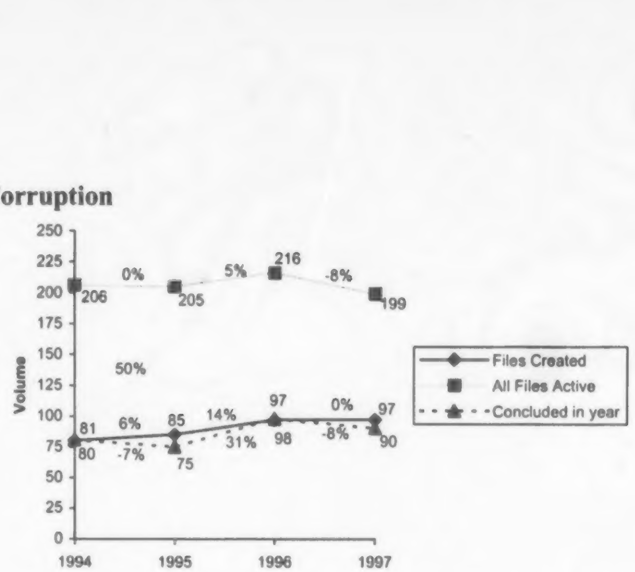
Source: RCMP Economic Crime MIS III. Query run before 4/7/98. Represents OSR Codes: AB53 Fraud cheques; AB55 Other frauds; AB57 Real estate fraud; AB58 Frauds (380 CCC).

Currency Counterfeiting



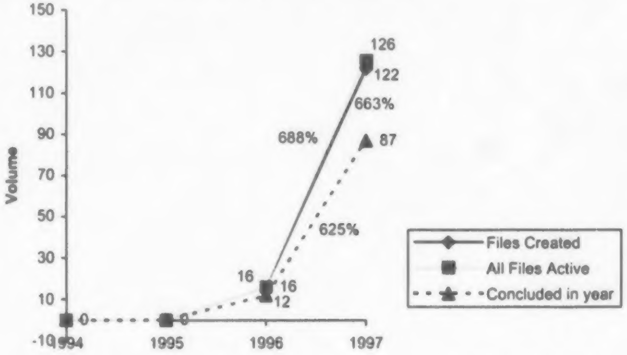
Source: RCMP Economic Crime MIS III. Query run as of 4/7/98. Represents OSR Codes: AC24 Counterfeit currency.

Corruption



Source: RCMP Economic Crime MIS III. Query run before 4/7/98. Represents OSR Codes: AB62 Criminal breach of trust; AC62 Corruption; AC63 Bribing government official; AC67 Breach of trust by public official.

Internet Crime and Computer Search

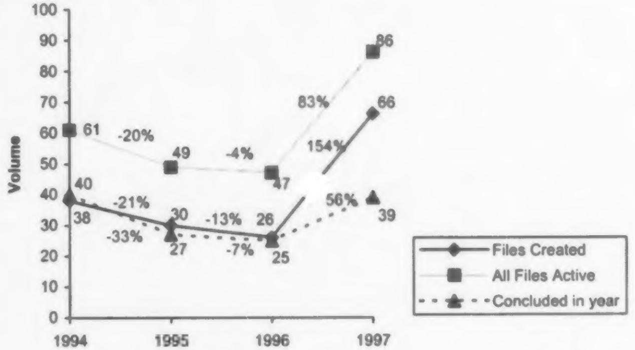


Source: RCMP Economic Crime MIS III. Query run as of 4/7/98.

Represents OSR Codes: DK42 Crime involving the internet; DK43 Computer search and analysis.

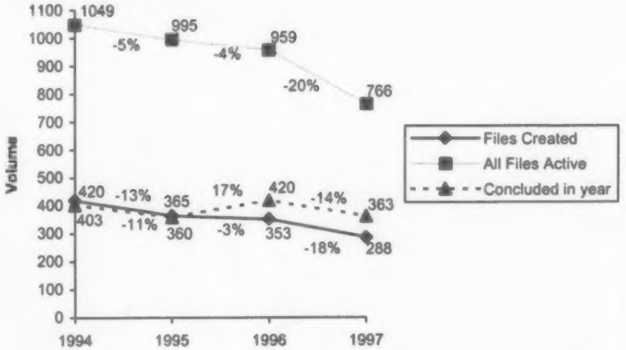
Note: Part of the 663% increase may be due to increased usage of the DK survey code, rather than stating an actual activity increase.

Payment Card Fraud



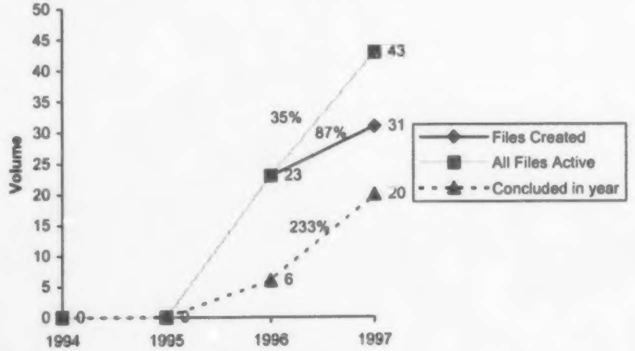
Source: RCMP Economic Crime MIS III. Query run before 4/7/98.
Represents OSR Codes: AB54 Credit card fraud; DK58 Counterfeit credit card.

Other Offences



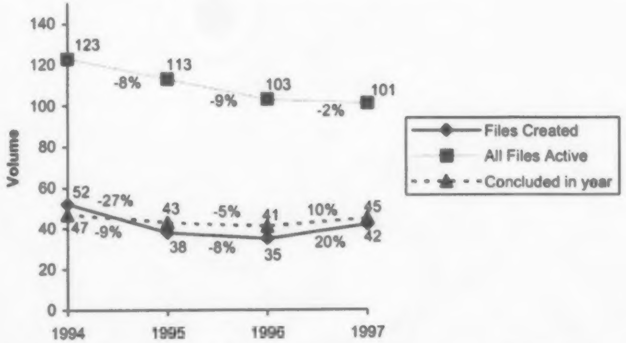
Source: RCMP Economic Crime MIS III. Query run as of 4/7/98.
Represents OSR Codes: AB26 Other theft >$5K; AB37 Other theft <$5K; AB59 Personation; AB60 Forgery; AB61 Uttering; AB63 Falsify books and records; AB65 Secret Commissions; AC64 Conspiracy.

MLAT Requests



Source: RCMP Economic Crime MIS III. Query run as of 4/7/98.
Represents OSR Codes: DK99 MLAT Requests.

Federal Statutes—Economic Crime Mandate



Source: RCMP Economic Crime MIS III. Query run as of 4/7/98.
Represents OSR Codes: AF02 Bank Act; AF03 Canada Election Act; AF21 Employment Insurance Act; AF25 Small Business Loan Act; AF36 Tax Rebate Discounting Act; AF37 Advance Payment for Crops Act.

Appendix J

Bibliography

Bibliography

American Bankers Association. **Public Relations News Page** on Debit Card and Credit Cards, (www.aba.com)

American Sociological Review. **"Is White Collar Crime' Crime,"** American Sociological Review, 10, pp132-139, 1945.

Anderson, Ross, and Kuhn, Markus. **Tamper Resistance - a Cautionary Note,** Cambridge University Computer Laboratory, Cambridge UK, 1996.

AUSTRAC. **Annual Report: 1996-97**, Commonwealth of Australia, Canberra, 1997.

Australian Defence Studies Centre. **Transnational Crime: A New security Threat?**, edited by John Ciccarelli, published by then Australian defence Force Academy and the University of NSW, 1996.

Australian Federal Police. **Annual Report: 1996-97**, Commonwealth of Australia, Canberra, 1997.

Australian Federal Police. **Miscellaneous documents**, Commonwealth of Australia, Canberra, 1997.

Australian Institute of Criminology. **"The Future of Crime Control,"** Australian Institute of Criminology Trends and Issues #63, 1996b.

Australian Office of Strategic Crime Assessments. **"Occasional Papers"**, discussion outlines and non-protected internal working documents, 1997.

Bank of Canada. Table B4—**Statistics Pertaining to Counterfeit Bank of Canada Notes**, Spring 1998

Bayley, David and Shearing, Clifford. **"The Future of Policing,"** Law and Society Review, Vol. 30, No. 3, 1996.

Bayley, David. **Police For The Future**, Oxford University Press, New York, 1994.

Better Business Bureau. **New Survey indicates how to increase consumer confidence in shopping online**, (www.bbb.org), 1998.

Blackburn, Wayne. **"Fraud on the Internet"**, CGA Magazine, October 1997 (www.cga-canada.org/CGAMagazine/oct97/fraud_e.htm)

Blum, Jack. **Enterprise Crime: Financial Fraud in International Interspace**, Working Group on Organized Crime, National Strategy Information Center, Washington DC June. Reported on in Trends in Organized Crime, Vol.3, No.1, .115, Fall 1997.

Brunker, Mike. **Hackers Penetrate Pentagon Network**, MSNBC, (www.msnbc.com/news), April 22, 1998.

Business Software Alliance. **Overview, Global Software Piracy Report, Facts and Figures 1994 - 1996**, (www.bsa.org).

Calavita, Kitty, Pontell, H. and Tillman, R. **Big Money Crime: Fraud and Politics in the Savings and Loan Crisis**, University of California press, Berkeley, 1997.

Canadian Bankers Association. **Credit Card Fraud Newsletter**, (www.cba.ca), April 1998.

Canadian Bankers Association. **Credit Card and Credit Card Fraud Statistics**, 1998 (www.cba.ca)

Canadian Direct Marketing Association. **Annual Fact Book**, Fifth Edition, Canadian Direct Marketing Association, 1996.

Canadian Direct Marketing Association. **CDMA Welcomes Amendments to the Competition Act**, (www.cdma.org), 1998.

Canadian Police Research Centre. **Annual Report: 1996-1997**, Minister of Supply and Services Canada, Ottawa, 1997.

Canadian Police Research Centre. **Various minutes and excerpts from reports** supplied by the CPRC, 1998.

Canadian Police Research Centre: Public Safety Network. **Law Enforcement Support Programs**, 1998 and **Internet Skills for Law Enforcement Professionals**, 1998.

Carter David, L. **"Emerging Trends in International Organized Crime."** Paper presented at the 19th International Asian Organized Crime Conference, Orlando, Florida, 1997.

CERT Coordination Center. **1997 Annual Report** (summary), Carnegie Mellon, University, 1998 (www.cert.org/annual_rpts/cert_rpt_97.html)

CGA Magazine. **Fraud on the Internet**, (www.cga-canada.org), 1997.

Cnet. **How Big is E-Commerce**, (www.cnet.com), 1997.

Computer Security Institute. **1998 CSI/FBI Computer Crime Security Survey**, (www.gocsi.com).

Criminal Intelligence Service Canada (CISC). **Organized Crime Workshop Proceedings**, June, Ottawa, Canada, 1997.

Csonka Peter. **"Combatting Economic and Organized Crime: The Council of Europe Perspective,"** paper produced by the Council of Europe, 1997.

CTIA. **Wireless Telephone Fraud Frequently Asked Questions**, www.wow-com.com/professional/fraud/Ffaqs.cfm)

Cybersource. **Credit Card Fraud Against Merchants (White Paper)**, (www.cybersource.com), 1998.

Davis, R.W.K, & Hutchinson, S.C. **Computer Crime in Canada: An Introduction to Technological Crime and Related Legal Issues**, Toronto: Carswell Publishing, 1997.

Doob, Anthony N. **Thinking About Police Resources**, (edited) Centre of Criminology, Univ. of Toronto, Toronto, 1993.

Doob, Tony (editor) **"Back from Wonderland, or towards the rational use of police resources,"** in Thinking about Police Resources, Research Report #26, Centre of Criminology, University of Toronto, 1993.

Ericson, R.V. **"The Royal Commission on Criminal Justice System Surveillance,"** in M. McConville (ed) Criminal Justice in Crisis, London: Edgar Elgar, 1994.

Ericson, R.V. and Haggerty, Kevin. **Policing the Risk Society**, University of Toronto Press, Toronto, 1997.

Ericson, R.V. and Shearing, C.D. **"The Scientification of Police Work"** in G. Bohme and N. Stehr (eds). **The Knowledge Society: The growing Impact of scientific Knowledge on Social Relations**, pp 129-159. Dordrecht: D. Reidl publishing, 1986.

Ernst & Young International. **1st Annual Global Information Security Survey**, Information Systems Assurance and Advisory Services, United States. (www.eycan.com – It's not right), 1998.

European Commission. **"Organised Criminality in Europe: A Descriptive Analysis."** Paper prepared for the Europeon Conference for Judges and Senior Judges: "New

Ways of Organized Criminality and Extradition." Conference organized by the European Commission and the Consejo general del poder judicial, Barcelona Spain, December, 1997b.

FATF. **Report on Money Laundering Typologies**, Published by the Financial Action Task Force on Money Laundering, 1997-98.

FATF. **The Forty Recommendations**. Published by the Financial Action Task Force on Money Laundering, 1996.

Federal Bureau of Investigation, National Infrastructure Protection Centre. Response to Information Request, June 1, 1998.

Federal Bureau of Investigation. **Telemarketing Fraud: Senior Sentinel**, Washington DC, no date (www.fbi.gov/majcases/telefrad/telfrad.htm)

Federal Trade Commission. **Fighting Consumer Fraud: The Challenge and the Campaign**, Washington DC, January 1997.

Felten, Edward W., Balfanz, D., Dean, D., and Wallach, D.S. **Web Spoofing: An Internet Con Game**, Department of Computer Science, Princeton University, (www.securitymanagement.com), 1997.

Financial Times (London Edition). **"Plastic Card Fraud on the Increase Again"**, April 4, 1998

Florida Attorney General's Office. **Credit Card Fraud**, (legal.firm.edu/consumer/tips/tipcarfr.html)

Forrester Research. **Sizing Intercompany Commerce Report**, Cambridge, MA, July 1997 (www.forrester.com)

Freeh, Louis. **Speech by Louis J. Freeh, Director of the FBI**, 1997 International Computer Crime Conference, New York, NY, March 4, 1997.

General Accounting Office (GAO). **Identify Fraud**, Washington DC, May 1998, Report Number GGD-98-100BR and **Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking**, January 1998, Report # GGD-98-34.

Gips, Michael A., **"Where Has All the Money Gone?"**, Security Management Online, February 1998 (www.securitymanagement.com)

Gordon Robert, and Nelson, J. **"Crime, Ethnicity, and Immigration,"** in R. Silverman edited Crimes in Canadian Society, Harcourt brace, Toronto, 1996.

Grabosky, P.N. **"The Changing Face of Crime Control,"** Transnational Crime: A New Security Threat, edited by John Ciccarelli, Australian Defence Studies Centre, 1996.

Grabosky, P.N. and Smith, R.G. "Telecommunications and Crime: Regulatory Dilemmas," in Law and Policy, 19, 3, July 1997.

Grant, Susan. **Fraudulent Schemes on the Internet: Remarks to Senate Permanent Committee on Investigations**, National Fraud Information Center/Internet Fraud Watch Programs, Washington DC, 1988 (www.fraud.org/internet/intstat.htm)

HM Inspectorate of Constabulary. **What Price Policing? A Study of Efficiency and Value for Money in the Police Service**, April 1998.

Howard, John D. **An Analysis of Security Incidents on the Internet**, (www.cert.org), 1997.

Industry Canada. **A Cryptography Policy Framework for Electronic Commerce**, (strategis.ic.gc.ca), 1998.

Industry Canada. **Report of the Canada-United States Working Group on Telemarketing Fraud**, Competition Bureau, (strategis.ic.gc.ca), 1997.

Industry Canada. **Information and Communications Technologies: Statistical Review 1990-1996**, Spectrum, Information Technologies and Telecommunications Sector, Ottawa, February 1998 (strategis.ic.gc.ca/infotech)

Industry Canada. **The Telecommunications Service Industry's Contribution to the Canadian Economy**, in The Canadian Telecommunications Industry - 1990 to 1996, (strategis.ic.gc.ca), 1998.

International Data Corporation (IDC): **Dramatic Growth of Web Commerce - From $2.6 Billion in 1996 to more than $220 Billion by 2001"**, (press release promoting forecasts from IDC's Internet Commerce Market Model, May 1998) (www.idc.com/f/HNR/ic2001f.htm)

Johnson, Les. **The Rebirth of Private Policing**, London, Rouledge Press, 1992.

Kabay, M.E. **ICSA White Paper on Computer Crime Statistics**, (www.ncsa.com), 1998.

KPMG Investigation and Security Inc. **1995-1998 Fraud Survey Reports**, Toronto.

Levi, Michael. **Regulating Fraud: White-Collar Crime and the Criminal Process**, Tavistock Publications, London, 1987.

Marshall, Ineke Haen. **Minorities, Migrants, and Crime: Diversity and Similarities Across Europe and the United States**, Sage Publications, London, 1997.

McFarlane John. **"Transnational Crime as a Security Issue"**, unpublished paper, 1997.

Metro Toronto Police Fraud Squad. **1997 Unit Strategies: Year End Report**, 1997.

Metro Toronto Police Fraud Squad. **FIAT System Ad Hoc Reports**, March 9, 1998.

Metro Toronto Police Fraud Squad. **Various organizational information** provided by the Metro Toronto Police Fraud Squad, 1998.

Metro Toronto Police Service. **Statistical Report**, 1996.

Metro Toronto Police. **Annual Report**, 1996 and **Fraud Squad Review**, 1996.

Milstone, Erik. **"Subscription Fraud Looms"**, Wireless Week, October 6, 1997.

Ministère de l'Intérieur, France. **Senior Experts on Transnational Organized Crime**, University of Toronto Library and the G8 Research Group at the University of Toronto, (http://utl2.library.utoronto.ca/disk1/www/documents/g7/40pts.htm),1996.

Morgan Stanley. **The Internet Retailing Report**, New York, (www.ms.com), 1997.

Myers, Willard. **"Orb Weavers–The Global Webs: The Structure and Activities of Transnational Ethnic Chinese Criminal Groups,"** Transnational Organized Crime, Winter, #4, vol.1, pp1-36, 1995.

National Fraud Information Center. (www.fraud.org).

Naylor, R.Tom. **"From Underworld to Underground: Enterprise 'Informal Sector' Business and the Public Policy Response,"** Crime, Law and Social Change, 24: 79-150, Kluwer Academic Publisher, Netherlands, 1996.

NASAA. **"With DOW over 9000, Investors Urged to be on the Guard for Fraud"**, Press Statement, 1998 (www.nasaa.org/investoredu/informed investor/dow9000f.html)

NASDAQ. **1997 Annual Report** and **1997 Fact Book: Market Data** (www.nasdaqnews.com)

O'Malley, Pat. **"Politicing, Politics, and Postmodernity."** Paper presented at York University, Fall, 1996.

Ontario Provincial Police, **Anti-Rackets Section Overview** provided by the OPP AntiRackets Section, 1998.

Ontario Provincial Police, **Anti-Rackets Section Occurrence Statistics—1994, 1995, 1996** provided by the OPP, May 1998.

Owens, Charles L., **Computer Crimes and Computer Related or Facilitated Crimes**, Statement to the Subcommittee on Technology, Terrorism and Governmental Information, Committee on the Judiciary, FBI, Washington DC, March 1997 (www.fbi.goc/archives/congress/compcrm.htm)

Pearce F and Snider L. (editors) **"Serious Fraud in Britain: Criminal Justice Versus Regulation,"** in Corporate Crime: Contemporary Debates, U of T Press, 1995.

Phillips, Colin (Chief Constable of Cumbria). **"Transnational Crime: Recent Trends and Future Prospects: Developments in UK Policing,"** Paper given at the Edinburgh Conference on Transnational and International Crime, May 15-17, 1997.

Phonebusters: **National Task Force Combating Telemarketing Fraud**, North Bay, Ontario (www.gov.on.ca/phonebusters)

Plecas, Darryl and J. Evans and Y. Dandurand. **Migration and Crime: A Canadian Perspective**, paper presented at the International Conference on Migration and Crime: Global and Regional Problems and Responses," Courmayeur Italy, 1996.

Price Waterhouse LLP. **Forensic Investigations: White Collar Crimes**.

Purton, Peter. **"Fraud and Theft",** Financial Times, June 10, 1998

RCMP, **ad hoc reports** from OSR/MIS III, June, 1998.

RCMP, **Commercial Crime Investigators Course**, Course Training Standard, Training Program and Development Branch, Ottawa. June, 1992.

RCMP, Economic Crime Branch. **Economic Crime Program Mandate Study**, Prepared by George P. Kaine, OIC Economic Crime Branch and approved by René Charbonneau, director, Federal Services, 1998.

RCMP, **Minimum Standards of Policing Study—Phase I**, (chapter on Commercial Crime Section), Corporate Management Branch-"D" Division , 1995.

RCMP, **Operational Statistics Reporting (OSR) Scoring Guide**, Published by Technical Information Services Section, Informatics Directorate, Ottawa, 1997.

RCMP, **Operational Statistics Reporting (OSR) System Index and Tables**, Prepared by Technical Information Services Section, Informatics Directorate, Ottawa, 1997.

RCMP, Vancouver Commercial Crime Section, **"Capital Costing Relating to Hardware Purchases for VCCs"**, Internal Memorandum, February 23, 1998.

RCMP Web Site. **Counterfeiting** (www.rcmp-grc.gc.ca/ntml/counter.htm)

Savona, Ernesto. **"Learning from Criminals to Combat Them: The Interdependence Among Fraud, Money Laundering and Corruption in Europe**," Transcrime Paper #14, prepared for the 8th International Anti-Corruption Conference, Lima Peru, September, 1997a.

Scams on the Net (700) (www.advocacy-net.com).

Schroeder, Michael. **"Penny Stock Fraud is Again on the Resurgence"**, Wall Street Journal, September 4, 1997

Serious Fraud Office. **Annual Report:** United Kingdom, London, 1993-1997.

Shearing, C. and Stenning, P. **Private Policing**, London, Sage Publications, 1987.

Sliter, John. **A Policy Review of the Role of The Royal Canadian Mounted Police in Securities Fraud Enforcement**, MBA, Simon Fraser University, 1994.

Slotter, Keith. **"Plastic Payments: Trends in Credit Card Fraud"** in FBI Law Enforcement Bulletin, June 1997 (www.fbi.gov/leb/june971.htm)

Smith, Russel. **National Fraud Statistics**, Australian Heads of Fraud Conference, 1997.

Solicitor General. **Annual Statement on Organized Crime**, The Hon. Andy Scott, House of Commons November 12, 1997.

Stanley, Christopher. **"Speculations on the Conflict of Discourses: Finance, Crime and Regulation,"** in the Journal of Financial Regulation and Compliance, Vol.4, #3, pp239-254, 1996.

Statistics Canada. **"Fraud in Canada 1977-1996,"** Canadian Centre for Justice Statistics, 1998.

Sutherland, Edwin H. **White Collar Crime**, NY Dryden Press, 1949.

Thomas, D. **"Criminality Among the Foreign Born: Analysis of Federal Prison Population,"** Ottawa: Immigration and Employment Canada, 1992.

Toronto Stock Exchange and Ontario Securities Commission. **Setting New Standards:** Mining Standards Task Force Interim Report, June 1998

Trofymowych, Delaine. **"Private Policing in Canada: A Review,"** Working paper prepared for the Department of the Solicitor General, 1993.

TSE, Mse, ASE, VSE and CDN. **Annual Reports** and **Market Summaries**

U.S. Department of Justice: Criminal Division. **Various background documents** provided by the Infotech Training Working Group (ITWG), 1998.

U.S. Department of Justice: Federal Bureau of Investigations. **White-Collar Crime: Facts and Cases**, 1996.

U.S. Federal Trade Commission. **Fighting Consumer Fraud: The Challenge and the Campaign**, January 1997. (www.ftc.gov/reports/Fraud/index.htm)

UK, Home Office. **International, National, Interforce Crime**, Study Commissioned by the Association of Chief Police Officers (ACPO). Prepared by the Police Research Group, 1996.

United Nations, **The United Nations Manual on the Prevention and Control of Computer-related Crime**. International Review of Criminal Policy, Nos. 43 and 44 (date unknown).

UpStartMagazine. **Insecure Transactions**, (www.upstartmagazine.com), 1997.

Visa Card. **Visa is Your Most Profitable Payment Card Option** (www.visa.com).

Web site information to check for DNS entries and domain names: www.internic.net, www.netnames.net, www.alldomains.com

Web site with computer crime information "do-it-yourself": www.hackershomepage.com, www.tsc-global.com, www.fc.net/phrack, www.2600.com

Web site with computer crime information on protection: www.10pht.com, www.nmrc.org, www.infowar.com, www.info-sec.com